

REPEAT PROCESSOR AND ITS METHOD

Patent number: JP2003229900
Publication date: 2003-08-15
Inventor: NAGASHIMA MASARU
Applicant: MITSUBISHI ELECTRIC CORP
Classification:
 - **international:** H04L12/46; H04L12/56; H04L12/46; H04L12/56; (IPC1-7): H04L12/56; H04L12/46
 - **European:**
Application number: JP20020026581 20020204
Priority number(s): JP20020026581 20020204

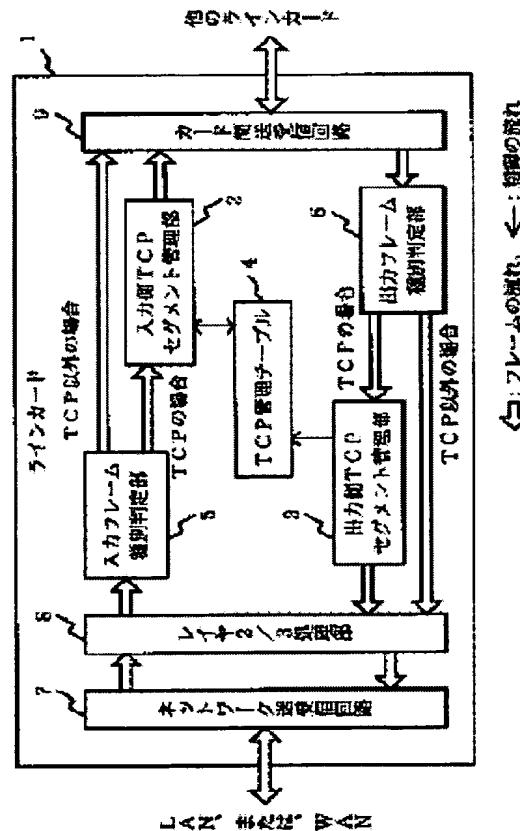
[Report a data error here](#)

Abstract of JP2003229900

PROBLEM TO BE SOLVED: To improve the utilization efficiency of a network by canceling invalid packets such as a packet of data omission.

SOLUTION: In a plurality of line cards 1 loaded in an IP router, a TCP management table 4 stores the sequence number of a packet to be received next as a Seq number and stores the sequence number of a latest packet received by the packet receiving side as an Ack number and an input side TCP segment management part 2 receives a packet transmitted by a LAN or the like through a network transmitting/receiving circuit 7 or the like, compares the sequence number of the received IP packet with the Seq number and the Ack number stored in the table 4, and when the value of the sequence number is not less than the Ack number and not more than the Seq number, updates the Seq number stored in the table 4 to the sequence number of the packet to be received next, transmits the sequence number to another line card 1 through an inter-card transmitting/receiving circuit 9, and cancels the received packet.

COPYRIGHT: (C)2003,JPO



Data supplied from the **esp@cenet** database - Worldwide

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-229900

(P2003-229900A)

(43)公開日 平成15年8月15日(2003.8.15)

(51)Int.Cl. ⁷	識別記号	F I	マーク一(参考)
H 04 L 12/56	2 0 0	H 04 L 12/56	2 0 0 Z 5 K 0 3 0
12/46		12/46	E 5 K 0 3 3
	1 0 0		1 0 0 R
	2 0 0		2 0 0 S

審査請求 未請求 請求項の数16 O.L (全26頁)

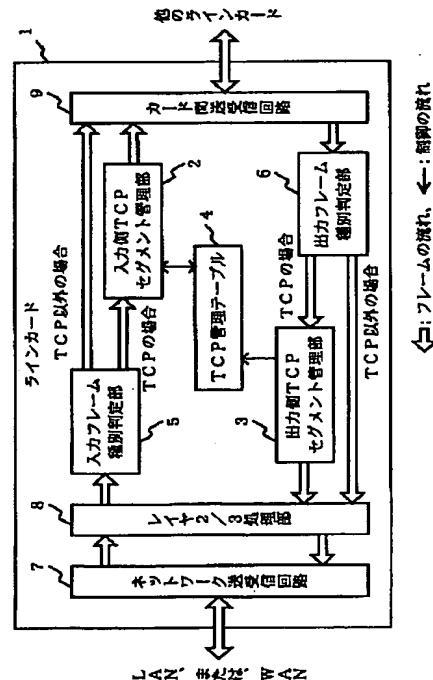
(21)出願番号	特願2002-26581(P2002-26581)	(71)出願人	000006013 三菱電機株式会社 東京都千代田区丸の内二丁目2番3号
(22)出願日	平成14年2月4日(2002.2.4)	(72)発明者	長島 勝 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
		(74)代理人	100099461 弁理士 溝井 章司 (外5名) Fターム(参考) 5K030 HA08 HC01 HC14 HD03 HD05 HD06 JA05 KA04 LA02 MB13 MB18 5K033 CB08 CC01 DA06 DB12 DB18

(54)【発明の名称】 中継処理装置及び中継処理方法

(57)【要約】

【課題】 データ抜け等の無効なパケットを廃棄し、ネットワークの利用効率を向上させる。

【解決手段】 I Pルータ内に複数枚実装されたラインカード1において、TCP管理テーブル4には次に受信するパケットのシーケンス番号がSeq番号として記憶され、パケットの受信側が受信した最新のパケットのシーケンス番号がAck番号として記憶されており、入力側TCPセグメント管理部2は、LAN等より送信されたパケットをネットワーク送受信回路7等を介して受信し、受信したIPパケットのシーケンス番号とTCP管理テーブル4内のSeq番号、Ack番号とを比較し、シーケンス番号の値がAck番号以上の値であってSeq番号以下の値である場合には、TCP管理テーブル4内のSeq番号を次に受信するパケットのシーケンス番号に更新してカード間送受信回路9を介して他のラインカードに送信し、その他の場合には受信したパケットを廃棄する。



【特許請求の範囲】

【請求項1】 それぞれに少なくとも一つ以上の通信装置を有する複数のネットワークに接続された中継装置内で、前記複数のネットワークのうち特定のネットワークに関する中継処理を行う中継処理装置であって、前記特定のネットワーク内の通信装置である特定ネットワーク通信装置から他のネットワーク内の通信装置である他ネットワーク通信装置に対して送信されたデータパケットであって、送信シーケンス番号として所定のシーケンス番号が付与されたデータパケットを順次受信する第一の通信処理部と、データパケットに対する中継処理の要否判断の基準となるシーケンス番号を判断基準シーケンス番号として記憶する通信管理テーブルと、前記第一の通信処理部によりデータパケットが受信される度に、受信された受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶された判断基準シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行う中継要否判断部と、前記中継要否判断部により中継処理の対象とされた受信データパケットを前記他ネットワーク通信装置に対して送信する第二の通信処理部とを有することを特徴とする中継処理装置。

【請求項2】 前記中継要否判断部は、受信データパケットを中継処理の対象とする度に、中継処理の対象とした受信データパケットの次に中継処理の対象となるデータパケットの送信シーケンス番号を次中継シーケンス番号として算出し、次中継シーケンス番号を算出する度に新たに算出した次中継シーケンス番号に更新しながら前記通信管理テーブルに次中継シーケンス番号を登録し、前記第二の通信処理部は、前記他ネットワーク通信装置がデータパケットを受信した場合に送達確認のために前記他ネットワーク通信装置から前記特定ネットワーク通信装置に対して送信された送達確認パケットであって、確認シーケンス番号として所定のシーケンス番号が付与された送達確認パケットを順次受信し、前記中継処理装置は、更に、前記第二の通信処理部により送達確認パケットが受信される度に新たに受信された送達確認パケットの確認シーケンス番号に更新しながら前記通信管理テーブルに確認シーケンス番号を登録する送達確認パケット管理部を有し、前記通信管理テーブルは、前記判断基準シーケンス番号として、前記中継要否判断部により最新に登録された次中継シーケンス番号と前記送達確認パケット管理部により最新に登録された確認シーケンス番号とを記憶し、前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットの送信シーケンス番号を、前記通信管理テーブルに記憶されている次中継シーケンス番号及び確認シーケンス番号のうち少なくともいずれか一つと比較して前記受信データ

タパケットについて中継処理の要否判断を行うことを特徴とする請求項1に記載の中継処理装置。

【請求項3】 前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶されている確認シーケンス番号とを比較し、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている確認シーケンス番号の値以上である場合に、前記受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶されている次中継シーケンス番号とを比較し、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている次中継シーケンス番号の値以下である場合に、前記受信データパケットを中継処理の対象とすることを特徴とする請求項2に記載の中継処理装置。

【請求項4】 前記中継要否判断部は、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている確認シーケンス番号の値未満であった場合及び前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている次中継シーケンス番号の値よりも大きい場合に、前記受信データパケットの廃棄を決定することを特徴とする請求項3に記載の中継処理装置。

【請求項5】 前記中継要否判断部は、中継処理の対象となった中継対象データパケットの送信シーケンス番号に前記中継対象データパケットのデータサイズを加算した値を前記次中継シーケンス番号として算出し、前記第二の通信処理部は、前記他ネットワーク通信装置が受信した受信済データパケットの送信シーケンス番号に前記受信済データパケットのデータサイズを加算した値を前記確認シーケンス番号とする送達確認パケットを受信することを特徴とする請求項2に記載の中継処理装置。

【請求項6】 前記通信管理テーブルは、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として記憶しており、前記中継要否判断部により最新に登録された次中継シーケンス番号と前記送達確認パケット管理部により最新に登録された確認シーケンス番号とを前記コネクション識別子情報に対応づけて記憶し、

前記第一の通信処理部は、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含むデータパケットを順次受信し、前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブル内で検索し、検索したコネクション識別子情報に対応づけられた次中継

シーケンス番号及び確認シーケンス番号のうち少なくともいずれか一つと前記受信データパケットの送信シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行うことを特徴とする請求項2に記載の中継処理装置。

【請求項7】 前記第一の通信処理部は、前記データパケットの受信に先立ち、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの設定のために前記特定ネットワーク通信装置より送信されたコネクション設定パケットを受信し、

前記通信管理テーブルは、前記第一の通信処理部により前記コネクション設定パケットが受信された場合に、受信された前記コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として記憶し、

前記第二の通信処理部は、前記コネクション設定パケットを前記他ネットワーク通信装置へ送信するとともに、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記コネクション設定パケットに対する応答として前記他ネットワーク通信装置より送信された応答コネクション設定パケットを受信し、

前記中継処理装置は、更に、前記第二の通信処理部により前記応答コネクション設定パケットが受信された場合に、前記応答コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブル内で検索し、対応するコネクション識別子情報が前記通信管理テーブル内に存在する場合に、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断するコネクション管理部を有することを特徴とする請求項1に記載の中継処理装置。

【請求項8】 前記第一の通信処理部は、所定の送信シーケンス番号が付与されたコネクション設定パケットを受信し、

前記通信管理テーブルは、前記第一の通信処理部により前記コネクション設定パケットが受信された場合に、受信された前記コネクション設定パケットの送信シーケンス番号に所定の値を加算した値を前記判断基準シーケンス番号として前記コネクション識別子情報に対応づけて記憶することを特徴とする請求項7に記載の中継処理装置。

【請求項9】 前記第二の通信処理部は、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの設定のために前記他ネットワーク通信装置より送信されたコネクション設定パケットを受

信し、受信した前記コネクション設定パケットを前記第一の通信処理部に転送し、前記第一の通信処理部は、前記第二の通信処理部より転送された前記コネクション設定パケットを前記特定ネットワーク通信装置へ送信するとともに、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記コネクション設定パケットに対する応答として前記特定ネットワーク通信装置より送信された応答コネクション設定パケットを受信し、

10 前記中継処理装置は、更に、前記第一の通信処理部により前記応答コネクション設定パケットが受信された場合に、前記応答コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として前記通信管理テーブルに登録するとともに、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断するコネクション管理部を有することを特徴とする請求項1に記載の中継処理装置。

20 【請求項10】 前記コネクション管理部は、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断した場合に、前記通信管理テーブル内の対応するコネクション識別子情報をコネクション確立フラグを設定することを特徴とする請求項7又は9に記載の中継処理装置。

【請求項11】 前記中継処理装置は、更に、一定周期ごとに前記通信管理テーブルを検査してコネクション識別子情報にコネクション確立フラグが設定されているか否かを確認し、コネクション確立フラグが設定されていないコネクション識別子情報を前記通信管理テーブルから削除するコネクション確認部を有することを特徴とする請求項10に記載の中継処理装置。

【請求項12】 前記第一の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの切断のために前記特定ネットワーク通信装置より送信されたコネクション切断パケットを受信し、

40 前記コネクション管理部は、前記第一の通信処理部により前記コネクション切断パケットが受信された場合に、前記コネクション切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする請求項7又は9に記載の中継処理装置。

【請求項13】 前記第一の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信

通信コネクションの強制切断のために前記特定ネットワーク通信装置より送信されたコネクション強制切断パケットを受信し、

前記コネクション管理部は、前記第一の通信処理部により前記コネクション強制切断パケットが受信された場合に、前記コネクション強制切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする請求項7又は9に記載の中継処理装置。

【請求項14】前記第二の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの強制切断のために前記他ネットワーク通信装置より送信されたコネクション強制切断パケットを受信し、

前記コネクション管理部は、前記第二の通信処理部により前記コネクション強制切断パケットが受信された場合に、前記コネクション強制切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする請求項7又は9に記載の中継処理装置。

【請求項15】前記中継要否判断部は、TCP (Transmission Control Protocol) プロトコルを用いるデータパケットについて中継処理の要否判断を行うことを特徴とする請求項1に記載の中継処理装置。

【請求項16】それぞれに少なくとも一つ以上の通信装置を有する複数のネットワークに接続された中継装置内で、前記複数のネットワークのうち特定のネットワークに関する中継処理を行う中継処理方法であって、前記特定のネットワーク内の通信装置である特定ネットワーク通信装置から他のネットワーク内の通信装置である他ネットワーク通信装置に対して送信されたデータパケットであって、送信シーケンス番号として所定のシーケンス番号が付与されたデータパケットを順次受信する第一の通信処理ステップと、

データパケットに対する中継処理の要否判断の基準となるシーケンス番号を判断基準シーケンス番号として記憶する通信管理ステップと、

前記第一の通信処理ステップによりデータパケットが受信される度に、受信された受信データパケットの送信シーケンス番号と前記通信管理ステップにより記憶された判断基準シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行う中継要否判断ステップと、

前記中継要否判断ステップにより中継処理の対象とされた受信データパケットを前記他ネットワーク通信装置に

対して送信する第二の通信処理ステップとを有することを特徴とする中継処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ルータ装置に用いられるTCP (Transmission Control Protocol) プロトコルを使用したIPパケットの管理技術に関する。

【0002】

10 【従来の技術】図19は、例えば、特開平11-27317号公報に示された従来のルータである。図19において、200はIPルータ、201は中継判定処理手段、202は経路制御データベース手段、203はフラグメント識別用記憶領域、204～205はネットワークインターフェース、206～208はネットワーク、209～210はネットワークに接続した局、211は他のIPルータ、220～229は局が送出したフラグメントされたIPパケットである。

【0003】このようなネットワークにおいて、局A209が局B210に宛てて、ネットワークに10個のフラグメントされたIPパケット220～229を送信した場合、従来のルータ200では、ネットワークインターフェースA204によってフラグメントされたIPパケット220～229を受信すると、経路制御データベース手段202により、宛先アドレスである局B210がどのネットワークに属するかを調べ、中継判定処理手段201により、該当するネットワークインターフェースB205へ送出する。

【0004】ルータ200は、内部のバッファ不足等により、フラグメントされたIPパケット220～229を中継できない場合、中継判定処理手段201により、そのIPパケットのIPヘッダから、送信元IPアドレス、宛先IPアドレス、及び、IDENTフィールド（このIDENTフィールドはIPパケットの各フラグメントの識別用として用いられる）の内容をフラグメント識別用記憶領域に保存して、IPパケットを廃棄する。また、後続のフラグメントされたIPパケットが、フラグメント識別用記憶領域203に保存されている内容と一致する場合に、既に先行するIPパケットが廃棄されているので、中継する必要がないと判断して、そのIPパケットを廃棄する。

【0005】

【発明が解決しようとする課題】上記のような従来のルータ200では、フラグメントされたIPパケット内の一部のIPパケットを自身で廃棄した場合しか後続のフラグメントされたIPパケットを廃棄できないという問題がある。他のルータで、フラグメントされたIPパケット内的一部のIPパケットが廃棄された場合には自ルータはこの廃棄されたIPパケットを検出できない。そのため、後続する無効なデータを含むIPパケットがネ

7
ネットワーク上を流れてしまい、ネットワーク全体の利用効率は十分に改善されない。

【0006】この発明は、上述のような課題を解決するためになされたものであり、第一の目的は、トランスポート層にTCPプロトコルを使用して通信されるユーザデータ(TCPセグメント)を管理する機能を実装することにより、データ抜けや重複による無効なトラフィックを検出して廃棄することにある。第二の目的は、無効なトラフィックの中継を削減することにより、ネットワークにおける輻輳を減らし、ネットワーク全体の利用効率を向上させることにある。

【0007】

【課題を解決するための手段】本発明に係る中継処理装置は、それぞれに少なくとも一つ以上の通信装置を有する複数のネットワークに接続された中継装置内で、前記複数のネットワークのうち特定のネットワークに関する中継処理を行う中継処理装置であって、前記特定のネットワーク内の通信装置である特定ネットワーク通信装置から他のネットワーク内の通信装置である他ネットワーク通信装置に対して送信されたデータパケットであって、送信シーケンス番号として所定のシーケンス番号が付与されたデータパケットを順次受信する第一の通信処理部と、データパケットに対する中継処理の要否判断の基準となるシーケンス番号を判断基準シーケンス番号として記憶する通信管理テーブルと、前記第一の通信処理部によりデータパケットが受信される度に、受信された受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶された判断基準シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行う中継要否判断部と、前記中継要否判断部により中継処理の対象とされた受信データパケットを前記他ネットワーク通信装置に対して送信する第二の通信処理部とを有することを特徴とする。

【0008】前記中継要否判断部は、受信データパケットを中継処理の対象とする度に、中継処理の対象とした受信データパケットの次に中継処理の対象となるデータパケットの送信シーケンス番号を次中継シーケンス番号として算出し、次中継シーケンス番号を算出する度に新たに算出した次中継シーケンス番号に更新しながら前記通信管理テーブルに次中継シーケンス番号を登録し、前記第二の通信処理部は、前記他ネットワーク通信装置がデータパケットを受信した場合に送達確認のために前記他ネットワーク通信装置から前記特定ネットワーク通信装置に対して送信された送達確認パケットであって、確認シーケンス番号として所定のシーケンス番号が付与された送達確認パケットを順次受信し、前記中継処理装置は、更に、前記第二の通信処理部により送達確認パケットが受信される度に新たに受信された送達確認パケットの確認シーケンス番号に更新しながら前記通信管理テーブルに確認シーケンス番号を登録する送達確認パケット

管理部を有し、前記通信管理テーブルは、前記判断基準シーケンス番号として、前記中継要否判断部により最新に登録された次中継シーケンス番号と前記送達確認パケット管理部により最新に登録された確認シーケンス番号とを記憶し、前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットの送信シーケンス番号を、前記通信管理テーブルに記憶されている次中継シーケンス番号及び確認シーケンス番号のうち少なくともいずれか一つと比較して前記受信データパケットについて中継処理の要否判断を行うことを特徴とする。

【0009】前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶されている確認シーケンス番号とを比較し、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている確認シーケンス番号の値以上である場合に、前記受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶されている確認シーケンス番号とを比較し、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている次中継シーケンス番号の値以下である場合に、前記受信データパケットを中継処理の対象とする

ことを特徴とする。

【0010】前記中継要否判断部は、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている確認シーケンス番号の値未満であった場合及び前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている次中継シーケンス番号の値よりも大きい場合に、前記受信データパケットの廃棄を決定することを特徴とする。

【0011】前記中継要否判断部は、中継処理の対象となつた中継対象データパケットの送信シーケンス番号に前記中継対象データパケットのデータサイズを加算した値を前記次中継シーケンス番号として算出し、前記第二の通信処理部は、前記他ネットワーク通信装置が受信した受信済データパケットの送信シーケンス番号に前記受信済データパケットのデータサイズを加算した値を前記確認シーケンス番号とする送達確認パケットを受信することを特徴とする。

【0012】前記通信管理テーブルは、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として記憶しており、前記中継要否判断部により最新に登録された次中継シーケンス番号と前記送達確認パケット管理部により最新に登録された確認シーケンス番号とを前記コネクション識別子情報に対応づけて記憶し、前記第一の通信処理部は、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含むデータパケットを順次受信し、前記中継要否判断部は、前記第一の通信

50

処理部によりデータパケットが受信される度に、受信データパケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブル内で検索し、検索したコネクション識別子情報に対応づけられた次中継シーケンス番号及び確認シーケンス番号のうち少なくともいずれか一つと前記受信データパケットの送信シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行うことを特徴とする。

【0013】前記第一の通信処理部は、前記データパケットの受信に先立ち、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの設定のために前記特定ネットワーク通信装置より送信されたコネクション設定パケットを受信し、前記通信管理テーブルは、前記第一の通信処理部により前記コネクション設定パケットが受信された場合に、受信された前記コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として記憶し、前記第二の通信処理部は、前記コネクション設定パケットを前記他ネットワーク通信装置へ送信するとともに、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記コネクション設定パケットに対する応答として前記他ネットワーク通信装置より送信された応答コネクション設定パケットを受信し、前記中継処理装置は、更に、前記第二の通信処理部により前記応答コネクション設定パケットが受信された場合に、前記応答コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブル内で検索し、対応するコネクション識別子情報が前記通信管理テーブル内に存在する場合に、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断するコネクション管理部を有することを特徴とする。

【0014】前記第一の通信処理部は、所定の送信シーケンス番号が付与されたコネクション設定パケットを受信し、前記通信管理テーブルは、前記第一の通信処理部により前記コネクション設定パケットが受信された場合に、受信された前記コネクション設定パケットの送信シーケンス番号に所定の値を加算した値を前記判断基準シーケンス番号として前記コネクション識別子情報に対応づけて記憶することを特徴とする。

【0015】前記第二の通信処理部は、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの設定のために前記他ネットワーク通信装置より送信されたコネクション設定パケットを受信

し、受信した前記コネクション設定パケットを前記第一の通信処理部に転送し、前記第一の通信処理部は、前記第二の通信処理部より転送された前記コネクション設定パケットを前記特定ネットワーク通信装置へ送信するとともに、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記コネクション設定パケットに対する応答として前記特定ネットワーク通信装置より送信された応答コネクション設定パケットを受信し、前記中継処理装置は、更に、前記第一の通信処理部により前記応答コネクション設定パケットが受信された場合に、前記応答コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として前記通信管理テーブルに登録するとともに、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断するコネクション管理部を有することを特徴とする。

【0016】前記コネクション管理部は、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断した場合に、前記通信管理テーブル内の対応するコネクション識別子情報にコネクション確立フラグを設定することを特徴とする。

【0017】前記中継処理装置は、更に、一定周期ごとに前記通信管理テーブルを検査してコネクション識別子情報にコネクション確立フラグが設定されているか否かを確認し、コネクション確立フラグが設定されていないコネクション識別子情報を前記通信管理テーブルから削除するコネクション確認部を有することを特徴とする。

【0018】前記第一の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションの切断のために前記特定ネットワーク通信装置より送信されたコネクション切断パケットを受信し、前記コネクション管理部は、前記第一の通信処理部により前記コネクション切断パケットが受信された場合に、前記コネクション切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする。

【0019】前記第一の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションの強制切断のために前記特定ネットワーク通信装置より送信されたコネクション強制切断パケットを受信し、前記コネクション管理部は、前記第一の通信処理部により前記コネクション強制切断パケットが受信された場合に、前記コネクション強制切断パケットに含

まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする。

【0020】前記第二の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの強制切断のために前記他ネットワーク通信装置より送信されたコネクション強制切断パケットを受信し、前記コネクション管理部は、前記第二の通信処理部により前記コネクション強制切断パケットが受信された場合に、前記コネクション強制切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする。

【0021】前記中継要否判断部は、TCP (Transmission Control Protocol) プロトコルを用いるデータパケットについて中継処理の要否判断を行うことを特徴とする。

【0022】本発明に係る中継処理方法は、それぞれに少なくとも一つ以上の通信装置を有する複数のネットワークに接続された中継装置内で、前記複数のネットワークのうち特定のネットワークに関する中継処理を行う中継処理方法であって、前記特定のネットワーク内の通信装置である特定ネットワーク通信装置から他のネットワーク内の通信装置である他ネットワーク通信装置に対して送信されたデータパケットであって、送信シーケンス番号として所定のシーケンス番号が付与されたデータパケットを順次受信する第一の通信処理ステップと、データパケットに対する中継処理の要否判断の基準となるシーケンス番号を判断基準シーケンス番号として記憶する通信管理ステップと、前記第一の通信処理ステップによりデータパケットが受信される度に、受信された受信データパケットの送信シーケンス番号と前記通信管理ステップにより記憶された判断基準シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行う中継要否判断ステップと、前記中継要否判断ステップにより中継処理の対象とされた受信データパケットを前記他ネットワーク通信装置に対して送信する第二の通信処理ステップとを有することを特徴とする。

【0023】

【発明の実施の形態】実施の形態1. 実施の形態1～6では、本発明に係る中継処理装置の例としてラインカードを用いる場合について説明する。図1は、ラインカードを複数枚実装したIPルータ10の構成を示し、図2は各ラインカードの内部構成を示している。なお、IPルータ10は中継装置に相当する。

【0024】図1に示すように、IPルータ10は、1

枚の制御カード11と、複数枚のラインカード1から構成される。実施の形態1では、ラインカード1を4枚実装した場合の構成例であり、IPルータ10内のラインカード1A～1Dは、それぞれLAN12、LAN13、WAN14、WAN15と接続されている。ラインカードA1AはLAN12に関する中継処理を、ラインカードB1BはLAN13に関する中継処理を、ラインカードC1CはWAN14に関する中継処理を、ラインカードD1DはWAN15に関する中継処理を、それぞれ行う。また、各ラインカードにとって、自己に接続するネットワークは特定のネットワークに相当し、他のラインカードに接続するネットワークは他のネットワークに相当する。例えば、ラインカードA1Aにとって、LAN12は特定のネットワークであり、LAN13は他のネットワークに相当する。また、特定のネットワーク内の通信装置は特定ネットワーク通信装置に相当し、他のネットワーク内の通信装置は他ネットワーク通信装置に相当する。例えば、ラインカードA1Aにとって、LAN12に接続されたクライアント18(端末A)は特定ネットワーク通信装置であり、LAN13に接続されたサーバ19(端末B)は他ネットワーク通信装置である。制御カード11とすべてのラインカード1A～1Dは、制御バス16で接続される。また、ラインカード1A～1D同士、及び、制御カード11と各ラインカード1A～1Dは、それぞれデータバス17で接続される。IPルータ10では、10組のデータバス17を有する。

【0025】次に、図2を参照してラインカードの構成を説明する。入力側TCPセグメント管理部2は、LAN12～13またはWAN14～15から受信したIPパケットの内、トランスポート層にTCPプロトコルを使用するIPパケットを受けて、TCP管理テーブル4の制御、及び、重複やデータ抜けが発生したIPパケットの廃棄を行う。なお、後述するように、入力側TCPセグメント管理部2には、中継要否判断部に相当する要素が含まれる。出力側TCPセグメント管理部3は、LAN12～13またはWAN14～15へ送出するIPパケットの内、トランスポート層にTCPプロトコルを使用するIPパケットを受けて、TCP管理テーブル4の制御を行う。TCP管理テーブル4には、入力側TCPセグメント管理部2による中継処理の要否判断に用いるシーケンス番号(判断基準シーケンス番号)が記憶されている。TCP管理テーブルは通信管理テーブルに相当する。

【0026】入力フレーム種別判定部5は、レイヤ2/3処理部8から渡されたIPパケットのトランスポート層のプロトコル種別を判別して、トランスポート層にTCPプロトコルを使用するIPパケットを入力側TCPセグメント管理部2に渡し、TCPプロトコル以外のプロトコルであればそのまま中継する。出力フレーム種別

判定部6は、他のラインカードから中継されたIPパケットのトランスポート層のプロトコル種別を判別して、トランスポート層にTCPプロトコルを使用するIPパケットを出力側TCPセグメント管理部3に渡し、TCPプロトコル以外のプロトコルであればそのままレイヤ2/3処理部8に渡す。

【0027】ネットワーク送受信回路7は、LAN12～13またはWAN14～15上の隣接ルータまたは端末との間で、IPフレームを送受信する。ネットワーク送受信回路7は、第一の通信処理部に相当する。レイヤ2/3処理部8は、LAN12～13またはWAN14～15から受信したIPフレームをデフレーム化して、IPプロトコル処理を行う。また、レイヤ2/3処理部8は、LAN12～13またはWAN14～15に送出するためにフレーム化を行う。カード間送受信回路9は、制御カード11または他のラインカードとの間で、データバス17を経由して、IPパケット20を送受信する。カード間送受信回路9は、第二の通信処理部に相当する。

【0028】図1において、端末Aと端末B間において、TCPプロトコル通信を行う場合を例とする。この時、端末Aをクライアント18、端末Bをサーバ19とする。

【0029】図3に、入力側TCPセグメント管理部2と出力側TCPセグメント管理部3で処理する、トランスポート層にTCPプロトコルを使用するIPパケット20の形式を示す。また、図4に、IPパケット20内のフラグビット32の詳細を示す。

【0030】IPパケット20は、ネットワーク層のIPヘッダ21、トランスポート層のTCPヘッダ22、ユーザデータ23の順で構成される。また、TCPプロトコルにおいて、TCPヘッダ22とユーザデータ23を合わせて、TCPセグメント24と称する。

【0031】IPヘッダ21は、プロトコル番号25、送信元IPアドレス26、及び、送信先IPアドレス27などから構成される。プロトコル番号25は、IPパケット20が運ぶ上位のプロトコルを示す識別番号であり、6であればTCP(トランスマッ션コントロール)プロトコルを、17であればUDP(ユーザデータグラム)プロトコルを示す。TCPセグメント24の場合は、6に設定されている。送信元IPアドレス26は、送信元を示す識別番号である。送信先IPアドレス27は、送信先を示す識別番号である。送信元IPアドレス26と送信先IPアドレス27は、IPプロトコルのバージョンによってサイズが異なり、IPv4では32ビット、IPv6では128ビットで表される。

【0032】TCPヘッダ22は、送信元ポート番号28、送信先ポート番号29、シーケンス番号30、確認応答番号31、及び、フラグビット32などから構成される。送信元ポート番号28は、送り元のポートの識別

番号である。送信先ポート番号29は、送り先のポートの識別番号である。送信元ポート番号28と送信先ポート番号29は、16ビットで表される。シーケンス番号30は、SYNビット34がONの場合に、接続時のシーケンス番号30の初期値を指定する。それ以外の場合は、このTCPセグメント24内のユーザデータ23が送信データ列中のどの位置にあるかを示す。このシーケンス番号30は、送信シーケンス番号に相当する。確認応答番号31は、ACKビット36がONの時のみ有効であり、次に受信を期待するシーケンス番号30を指定する。この確認応答番号31未満のシーケンス番号30を持つユーザデータ23は受信側で正常に受信されたことを示す。この確認応答番号31は、確認シーケンス番号に相当する。

【0033】フラグビット32は、TCPコネクション接続/切断、送達確認などのTCPセグメント24の種類を示す。フラグビット32には、FINビット33、SYNビット34、RSTビット35、ACKビット36などが存在する。本明細書では、1の場合をON、0の場合をOFFと記述する。

【0034】FINビット33は、ONの場合に、このTCPセグメント24の送り元からこれ以上送るユーザデータ23がないため、送り元はTCPコネクションを切断しようとしていることを示す。しかし、この状態では相手からのTCPセグメント24は受信可能である。この状態で、相手からFINビット33がONのセグメントを受信した時点で、TCPコネクションは削除される。SYNビット34は、ONの場合に、シーケンス番号30に初期値が設定されていることを示す。これは、TCPコネクション確立時に使用される。RSTビット35は、ONの場合に、このTCPセグメント24を送信した端末から、一方的かつ強制的にTCPコネクションを切断することを意味する。これは、再送信などの通常の方法で回復できないエラーが発生した場合などに使用される。通常、TCPセグメント24は、FINビット33、SYNビット34、RSTビット35の内、最大でも1個のビットのみONになる。

【0035】ACKビット36は、ONの場合に確認応答番号31が有効であることを示し、このTCPセグメント24に送達確認の情報を含むことを示す。

【0036】図5にTCP管理テーブル4を示す。このTCP管理テーブル4は、単一方向のTCPコネクション毎に、コネクション識別子41、Seq番号42、Ack番号43、及び、確立フラグ44を管理する。本明細書では、コネクション識別子41、Seq番号42、及び、Ack番号43を一組として、コネクション情報と称する。コネクション情報は、単一方向のTCPコネクション毎に存在する。

【0037】コネクション識別子41は、送信元ID45と送信先ID46を組合せたものである。送信元I

D 4 5 は、送信元のTCPソケットを示し、送信元ポート番号28と送信元IPアドレス26を組合せたものである。送信先ID46は、送信先のTCPソケットを示し、送信先ポート番号29と送信先IPアドレス27を組合せたものである。送信元ID45と送信先ID46は、IPプロトコルのバージョンによってサイズが異なり、IPv4では48ビット、IPv6では144ビットで表される。そのため、コネクション識別子41は、IPv4では96ビット、IPv6では288ビットで表される。

【0038】Seq番号42は、コネクション識別子41毎に、ラインカード1が次に受信するTCPセグメント24のシーケンス番号30を示す。なお、Seq番号42は、次中継シーケンス番号に相当する。Ack番号43は、コネクション識別子41毎に、ラインカード1が受信した最新の送達確認用TCPセグメント24の確認応答番号31を示す。なお、Ack番号43は確認シーケンス番号に相当する。また、次中継シーケンス番号(Seq番号42)及び、確認シーケンス番号(Ack番号43)をあわせて判断基準シーケンス番号とする。確立フラグ(コネクション確立フラグ)44は、TCPプロトコルで通信する端末間で、双方向のTCPコネクションが確立した場合にONに設定する。単方向のTCPコネクションが確立した時点ではOFFに設定する。また、一定周期で確立フラグ44を監視する際に、OFFであった場合はCHECKに変更する。

【0039】このように、TCP管理テーブル4で、單一方向のTCPコネクション毎に、ラインカード1が次に受信するTCPセグメント24のシーケンス番号30を管理することで、データの抜けを検出することができる。また、TCP管理テーブル4で、單一方向のTCPコネクション毎に、ラインカード1が受信した最新の送達確認用のTCPセグメント24の確認応答番号31を管理することで、TCPプロトコル通信における受信側が受け取り済みのTCPセグメント24を把握し、データの重複を検出することができる。また、本発明は、IPルータ10の個々のラインカード1に実装される機能であり、他のルータ装置の影響を受けない／与えないため、他社のルータ装置との相互接続性を保証することができる。

【0040】図6は、入力側TCPセグメント管理部2の詳細を示したものである。なお、図1と同等の機能を有する箇所には同一番号を付し説明を省略する。

【0041】入力側フラグビット判定部51は、IPパケット20内のフラグビット32を確認する。TCPコネクション確立の場合は、IPパケット20を入力側コネクション情報管理部54に渡す。なお、TCPコネクション確立の場合とは、TCPセグメント24のSYNビット34がONであり、かつ、FINビット33、RSTビット35がOFFである場合を指す。TCPコネ

クション切断の場合は、IPパケット20を入力側コネクション情報管理部54に渡す。なお、TCPコネクション切断の場合とは、TCPセグメント24のSYNビット34がOFFであり、かつ、FINビット33、または、RSTビット35のいずれかがONである場合を指す。データ送信の場合は、IPパケット20をフィルタ部52に渡す。なお、データ送信の場合とは、TCPセグメント24のFINビット33、SYNビット34、RSTビット35、ACKビット36のすべてがOFFである場合を指す。送達確認の場合は、カード間送受信回路9を経由して、他のラインカードに転送する。なお、送達確認の場合とは、TCPセグメント24のFINビット33、SYNビット34、RSTビット35のすべてがOFFであり、かつ、ACKビット36がONである場合を指す。

【0042】フィルタ部52は、データ送信の場合に、入力側フラグビット判定部51から渡されたTCPセグメント24に関して、TCP管理テーブル4を参照して、TCPセグメント24の正当性(連続するデータ列20であること)を確認し、中継処理の要否判断を行なう。

Seq番号更新部53は、データ送信の場合に、TCP管理テーブル4の該当するコネクション情報のSeq番号42の現在の値に、TCPセグメント24のデータサイズを加算し、次に受信する(次に中継処理の対象となる)TCPセグメント24のシーケンス番号30(次中継シーケンス番号)を算出する。また、コネクション情報のSeq番号42を、その算出値に更新する。フィルタ部52及びSeq番号更新部53は、中継要否判断部に相当する。入力側コネクション情報管理部54は、コネクション確立／切断時に、TCPセグメント24からコネクション情報を生成して、TCP管理テーブル4に登録、または、TCP管理テーブル4から削除する。入力側コネクション情報管理部54は、後述する出力側コネクション情報管理部63とともに、コネクション管理部に相当する。

【0043】コネクション確認部55は、一定周期でTCP管理テーブル4の確立フラグ44を監視し、2周期分(一定周期をTとした場合は2T)を経過しても、確立フラグ44がONでない場合、そのコネクション情報をTCP管理テーブル4から削除する。

【0044】図7は、出力側TCPセグメント管理部3の詳細を示したものである。なお、図1と同等の機能を有する箇所には同一番号を付し説明を省略する。

【0045】出力側フラグビット判定部61は、IPパケット20内のフラグビット32を確認する。TCPコネクション確立の場合は、IPパケット20を出力側コネクション情報管理部63に渡す。TCPコネクション切断の場合には、IPパケット20を出力側コネクション情報管理部63に渡す。送達確認の場合は、IPパケット20をAck番号更新部62に渡す。それ以外の場合50

は、レイヤ2/3処理部8、及び、ネットワーク送受信回路7を経由して、他のラインカードに転送する。それ以外の場合とは、データ送信時が該当する。

【0046】Ack番号更新部62は、送達確認の場合に、TCPセグメント24の確認応答番号31を、TCP管理テーブル4の該当するコネクション情報のAck番号43に更新する。なお、Ack番号更新部62は、送達確認パケット管理部に相当する。出力側コネクション情報管理部63は、コネクション確立時に、TCPセグメント24からコネクション情報を生成して、TCP管理テーブル4に登録する。また、コネクション情報が既にTCP管理テーブル4に登録されており、かつ、対応する確立フラグ44がONでない場合は、ONに設定する。なお、出力側コネクション情報管理部63は、前述の入力側コネクション情報管理部54とともにコネクション管理部に相当する。

【0047】このように、入力側TCPセグメント管理部2において、TCP管理テーブル4でコネクション情報のSeq番号42を管理して、ラインカード1が次に受信するTCPセグメント24を予測することにより、データ抜けによる無効なトラフィックを削減することができる。これについては後述する。また、出力側TCPセグメント管理部3において、TCP管理テーブル4でコネクション情報のAck番号43を管理して、TCPプロトコル通信における受信側が受け取り済みのTCPセグメント24を把握することにより、入力側TCPセグメント管理部2でデータ重複による無効なトラフィックを削減することができる。これについては後述する。

【0048】実施の形態2. 本実施の形態では、実施の形態1で示したラインカード1の処理のうち、コネクション確立時の処理の詳細を説明する。

【0049】TCPコネクションを確立するために、TCPプロトコルで通信する端末間で、3ウェイハンドシェークと呼ばれる手順を行う。TCPコネクション確立を要求するためのTCPセグメント24は、SYNビット34がONに設定されている。本明細書では、このTCPセグメント24を、SYNセグメント(コネクション設定パケット)と称する。また、送達確認用のTCPセグメント24は、ACKビット36がONに、かつ、FINビット33とRSTビット35がOFFに設定されている。本明細書では、このTCPセグメント24を送達確認セグメント(送達確認パケット)と称する。

【0050】3ウェイハンドシェークの動作を図8を用いて説明する。なお、図8において、記述のないFINビット33、SYNビット34、RSTビット35、ACKビット36は、OFFに設定されていることを意味する。

【0051】まず、第一フェーズとして、クライアント18は、接続したいサーバ19のポート番号と、クライアント18の初期シーケンス番号を指定したSYNセグ

メント71を、サーバ19に対して送信する。このSYNセグメント71は、フラグビット32の内、SYNビット34のみがONに設定されている。

【0052】次に、第二フェーズとして、サーバ19は、サーバ19側の初期シーケンス番号を指定したSYNセグメント72を、クライアント18に対して送信する。このSYNセグメント72は、フラグビット32の内、SYNビット34とACKビット36のみがONに設定されている。また、確認応答番号31には、クライアント18からのSYNセグメント71のシーケンス番号30に1を加算した値が設定される。なお、第二フェーズのSYNセグメントは、第一フェーズのSYNセグメントに対応する応答として送信されており、応答コネクション設定パケットに相当する。

【0053】最後に、第三フェーズとして、クライアント18は、サーバ19からのSYNセグメント72に対して、送達確認のTCPセグメント73で応答する。このTCPセグメント73は、フラグビット32の内、ACKビット36のみがONに設定されている。また、確認応答番号31には、サーバ19からのSYNセグメント72のシーケンス番号30に1を加算した値が設定される。

【0054】ラインカード1では、TCPコネクションを確立するためのSYNセグメントの受信を起因として、TCP管理テーブル4に、コネクション情報を登録する。この処理は、SYNセグメントを発行した端末の種類(クライアント18、または、サーバ19)により、2種類の方法に分けられる。端末の種類は、フラグビット32のACKビット36の設定値から判断する。

30 ACKビット36がOFFであるSYNセグメント71の発行元はクライアント18、ACKビット36がONであるSYNセグメント72の発行元はサーバ19である。

【0055】実施の形態2では、クライアント18からのSYNセグメント71の受信を起因とした、コネクション情報の登録について説明する。つまり、本実施の形態では、クライアント18からのSYNセグメントを受信した場合のラインカードA1Aの処理について説明する。

40 【0056】この場合は、コネクション情報が有効になるまでに、2段階の処理を行う。第一段階で、3ウェイハンドシェークの第一フェーズのSYNセグメント71に基づき、TCP管理テーブル4にコネクション情報を登録する。この時、確立フラグ44はOFFのままである。第二段階で、3ウェイハンドシェークの第二フェーズのSYNセグメント72を受けた時点で、第一段階で登録したコネクション情報に対応する確立フラグ44をONにする。ラインカードA1Aでは、第一段階を入力側TCPセグメント管理部2で処理し、第二段階を出力側TCPセグメント管理部3で行う。

【0057】図9は、TCPコネクション確立の内、SYNセグメントによるコネクション情報の登録処理のフローチャートである。この図9は、実施の形態2の第一段階の処理である。但し、図9のフローチャートでは、ステップ91～ステップ93を除き、クライアント18からのSYNセグメント71と、サーバ19からのSYNセグメント72で同一処理を行う。そのため、図9の各ステップの説明では、SYNセグメント71とSYNセグメント72に共通な場合はSYNセグメントとして記述する。

【0058】入力側フラグビット判定部51は、TCPセグメント24からフラグビット32を抽出（ステップ81）し、SYNビット34の設定値から、TCPコネクション確立を要求するためのSYNセグメントであるか否かを判定する（ステップ82）。SYNビット34がONの場合はステップ83に進む。また、SYNビット34がOFFの場合は終了する。但し、入力側フラグビット判定部51に渡されたIPパケットは、4種類（TCPコネクション確立、TCPコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（TCPコネクション切断、データ送信、送達確認）の判定に進むことを意味する。実施の形態2では、クライアントからのSYNセグメント71は、SYNビットがONであるため、ステップ83に進む。

【0059】ステップ82でYesの場合は、入力側コネクション情報管理部54は、IPパケット20内の、送信元IPアドレス26、送信元ポート番号28、送信先IPアドレス27、送信先ポート番号29を組合せて、コネクション識別子41を生成する（ステップ83）。次に、生成したコネクション識別子41をキーとして、TCP管理テーブル4を検索（ステップ84）し、一致するコネクション識別子が既に登録されているか否かを確認する（ステップ85）。既にTCP管理テーブル4に登録されている場合は、新しい情報に更新するために、ステップ84で検出した情報（旧情報）をTCP管理テーブル4から削除する（ステップ86）。

【0060】既にTCP管理テーブル4に登録されているケースとしては、図8において、クライアント18がサーバ19にTCPコネクション確立を要求した際に、サーバ19が停止している場合がある。この時、クライアント18は、サーバ19からの応答がないため、コネクション確立タイムアウトにより、SYNセグメント71を再送することになる。

【0061】入力側コネクション情報管理部54は、まず、TCP管理テーブル4の空きエントリに、ステップ83で生成したコネクション識別子41を登録する（ステップ87）。次に、SYNセグメントからシーケンス番号30を抽出する（ステップ88）。なお、SYNセグメントにおけるシーケンス番号30は、送信先ID4

6で示される端末が、送信元ID45で示される端末のポートに送信するTCPセグメントにシーケンシャルに付与する番号の初期値になる。そして、シーケンス番号30に1を加算した値を、ステップ87で登録したコネクション識別子41に対応するSeq番号42に登録する（ステップ89）。また、シーケンス番号30の値を、ステップ87で登録したコネクション識別子41に対応するAck番号43に登録する（ステップ90）。

【0062】入力側コネクション情報管理部54は、最後に、TCPセグメント24のACKビット36の設定値を確認（ステップ91）し、ステップ87で登録したコネクション識別子41に対応する確立フラグ44を設定する。ACKビット36がOFFの場合は、確立フラグ44をOFFに設定する（ステップ92）。また、ACKビット36がONの場合は、確立フラグ44をONに設定する（ステップ93）。実施の形態2では、クライアント18からのSYNセグメント71は、ACKビット36がOFFであるため、確立フラグ44をOFFに設定する。

【0063】最後に、入力側コネクション情報管理部54で処理されたIPパケット20は、カード間送受信回路9を経由して、そのIPパケット20を送出すべきラインカード1B～1Dに転送される。

【0064】図10は、サーバ19からの第二フェーズのSYNセグメント72による、コネクション情報の有効化処理のフローチャートである。この図は、実施の形態2の第二段階の処理である。

【0065】出力側フラグビット判定部61は、TCPセグメント24からフラグビット32を抽出（ステップ101）し、SYNビット34の設定値から、SYNセグメントであるか否かを判定する（ステップ102）。SYNビット34がONの場合はステップ103に進む。また、SYNビット34がOFFの場合は終了する。但し、出力側フラグビット判定部61に渡されたIPパケットは、4種類（TCPコネクション確立、TCPコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（TCPコネクション切断、データ送信、送達確認）の判定に進むことを意味する。実施の形態2では、サーバ19からの第二フェーズのSYNセグメント72は、SYNビット34がONであるため、ステップ103に進む。

【0066】出力側コネクション情報管理部63は、IPパケット20内の、送信先IPアドレス27、送信先ポート番号29を組合せて、送信元ID45を生成する（ステップ103）。また、IPパケット20内の、送信元IPアドレス26、送信元ポート番号28を組合せて、送信先ID46を生成する（ステップ104）。そして、ステップ103で生成した送信元ID45と、ステップ104で生成した送信先ID46を組合

わせて、コネクション識別子41を算出する（ステップ105）。出力側コネクション情報管理部63では、入力側コネクション情報管理部54と異なり、IPパケット20内の送信元／送信先を反転して、コネクション識別子41を生成する。次に、生成したコネクション識別子41をキーとして、TCP管理テーブル4を検索（ステップ106）し、既に登録されているか否かを確認する（ステップ107）。登録されている場合はステップ108に進み、登録されていない場合はステップ109に進む。

【0067】ステップ107でYesの場合は、出力側コネクション情報管理部63は、ステップ106で検出したコネクション識別子41に対応する確立フラグ44をONに設定する（ステップ108）。この時点で、コネクション情報は有効になる。

【0068】最後に、出力側コネクション情報管理部63で処理されたIPパケット20は、レイヤ2／3処理部8に渡される（ステップ109）。

【0069】なお、図8とは逆の場合、すなわち、第一フェーズのSYNセグメントがサーバ19からクライアント18に対して送信され、第二フェーズのSYNセグメントがクライアント18からサーバ19に対して送信された場合は、第一段階において、ラインカードB1Bの入力側TCPセグメント管理部2がTCP管理テーブル4にコネクション情報を登録し、第二段階において、出力側TCPセグメント管理部3が第一段階で登録したコネクション情報に対応する確立フラグ44をONにする。

【0070】TCPプロトコル通信では、各端末はTCPセグメント24に付与するシーケンス番号30をそれぞれ別々に管理するため、TCP管理テーブル4を使用して、データ抜けやデータ重複による無効なトラフィックを検出するためには、単一方向のTCPコネクション単位で管理する必要がある。ラインカード1において、3ウェイハンドシェークの第一フェーズのSYNセグメント71の受信を起因として、TCP管理テーブル4にコネクション情報を登録することにより、クライアント18からサーバ19への方向に関して、TCPコネクション単位で管理することができる。

【0071】実施の形態2では、コネクション情報の登録と有効化を別のフェーズで行うため、有効でないコネクション情報がTCP管理テーブル4に登録される場合がある。例えば、前述した、図8において、クライアント18がサーバ19にTCPコネクション確立を要求した際に、サーバ19が停止している場合がある。この時、クライアント18は、SYNセグメント71を再送することになるが、無限に繰り返すのではなく、一定期間を超えた場合にはSYNセグメント71を再送するのを停止する。

【0072】このようなTCP管理テーブル4のリソー

スの浪費を防止するため、コネクション確認部55は、一定周期で、TCP管理テーブル4に登録されているすべてのコネクション情報の確立フラグ44を監視し、無効のコネクション情報を削除する。

【0073】図11は、コネクション情報の監視処理のフローチャートである。

【0074】コネクション確認部55は、一定周期ごとに起動し、TCP管理テーブル4の確立フラグ44を確認（ステップ111）し、確立フラグ44の値により分岐する（ステップ112）。確立フラグ44がONの場合は、ステップ115に進む。確立フラグ44がOFFの場合は、確立フラグ44をCHECKに設定する（ステップ113）。確立フラグ44がCHECKの場合は、該当するコネクション情報をTCP管理テーブル4から削除する（ステップ114）。その時点でTCP管理テーブル4に登録されているすべてのコネクション情報に対して、ステップ111～ステップ114の処理を行われるまで繰り返す（ステップ115）。

【0075】このように、定期的にTCP管理テーブル4に登録されているコネクション情報を監視し、無効であるコネクション情報を検出して削除することにより、TCP管理テーブル4のリソースの浪費を防止することができる。

【0076】実施の形態3、実施の形態3では、サーバ19からの第二フェーズのSYNセグメント72の受信を起因とした、コネクション情報の登録について説明する。この場合は、コネクション情報が有効になるまでに、1段階の処理を行う。この場合、3ウェイハンドシェークの第二フェーズのSYNセグメント72を受けた時点で、そのSYNセグメント72に基づき、TCP管理テーブル4にコネクション情報を登録すると同時に、そのコネクション情報に対応する確立フラグ44をONにする。

【0077】サーバ19からの第二フェーズのSYNセグメント72によるコネクション情報の登録処理は、ラインカードB1Bの入力側TCPセグメント管理部2で行う。フローチャートは図9と同様である。

【0078】実施の形態2との違いは、ACKビット36の値により、TCP管理テーブル4の確立フラグ44への設定値が異なることである。ステップ92～ステップ93のいずれを選択するかにある。実施の形態3では、サーバ19からのSYNセグメント72は、ACKビット36がONであるため、ステップ93に進み、確立フラグ44をONに設定する。

【0079】なお、図8とは逆の場合、すなわち、第一フェーズのSYNセグメントがサーバ19からクライアント18に対して送信され、第二フェーズのSYNセグメントがクライアント18からサーバ19に対して送信された場合は、ラインカードA1Aの入力側TCPセグメント管理部2がコネクション情報の登録処理を行い、

確立フラグをONにする。

【0080】前述したが、TCPプロトコル通信では、各末端はTCPセグメント24に付与するシーケンス番号30をそれぞれ別々に管理するため、TCP管理テーブル4を使用して、データ抜けやデータ重複による無効なトラフィックを検出するためには、單一方向のTCPコネクション単位で管理する必要がある。ラインカード1において、3ウェイハンドシェークの第二フェーズのSYNセグメント72の受信を起因として、TCP管理テーブル4にコネクション情報を登録することにより、サーバ19からクライアント18への方向に関して、TCPコネクション単位で管理することができる。

【0081】また、実施の形態2では、コネクション情報の登録からコネクション情報の有効化まで、コネクション情報が無効な期間が存在する。一方、実施の形態3では、一個のSYNセグメント72により、コネクション情報の登録とコネクション情報の有効化を同時にを行うため、コネクション情報が無効な期間が存在しない。

【0082】また、実施の形態2と実施の形態3により、TCPプロトコル通信を行う末端間の双方のTCPコネクションに関して、ラインカードA1A及びラインカードB1Bがそれぞれ片方向のTCPコネクションを管理するTCP管理テーブルを保有することができ、適切な通信パケット制御を行なうことができる。

【0083】実施の形態4。本実施の形態では、実施の形態1で示したラインカード1の処理のうち、コネクション切断時の処理の詳細を説明する。

【0084】TCPコネクションの切断を要求するためのTCPセグメント24には2種類ある。一つ目は、FINビット33がONに設定されたTCPセグメント24であり、本明細書では、FINセグメントと称する。二つ目は、RSTビット35がONに設定されたTCPセグメント24であり、本明細書では、RSTセグメントと称する。なお、FINセグメントは、コネクション切断パケットに相当し、RSTセグメントはコネクション強制切断パケットに相当する。実施の形態4では、前者のFINセグメントによるTCPコネクション切断を示す。また、実施の形態5では、後者のRSTセグメントによるTCPコネクション切断を示す。

【0085】FINセグメントによるTCPコネクション切断では、TCPプロトコルで通信する末端間で、4個のセグメントを使用して行う。TCPプロトコル通信は双方に独立して通信できるため、各方向が独立的にTCPコネクションを切断しなければならない。そのため、クライアント18とサーバ19は両方から、FINセグメントを発行して、TCPコネクション切断を要求する。

【0086】TCPコネクション切断の動作を図12を用いて説明する。なお、図12において、記述のないFINビット33、SYNビット34、RSTビット3

5、ACKビット36は、OFFに設定されていることを意味する。

【0087】第一に、クライアント18からのTCPコネクション切断の場合である。まず、第一フェーズとして、クライアント18は、切断したいサーバ19のポート番号を指定したFINセグメント121を、サーバ19に対して送信する。次に、第二フェーズとして、サーバ19は、クライアント18からのFINセグメント121に対する応答であるTCPセグメント122を、クライアント18に対して送信する。その場合、フラグビット32の内、ACKビット36のみがONに設定されている。また、確認応答番号31には、クライアント18が送信したFINセグメント121のシーケンス番号30に1を加算した値が設定される。

【0088】第二に、サーバ19からのTCPコネクション切断の場合である。まず、第一フェーズとして、サーバ19は、切断したいクライアント18のポート番号を指定したFINセグメント123を、クライアント18に対して送信する。次に、第二フェーズとして、クライアント18は、サーバ19からのFINセグメント123に対する応答であるTCPセグメント124を、サーバ19に対して送信する。その場合、フラグビット32の内、ACKビット36のみがONに設定されている。また、確認応答番号31には、サーバ19が送信したFINセグメント123のシーケンス番号30に1を加算した値が設定される。

【0089】但し、クライアント18からのTCPコネクション切断と、サーバ19からのTCPコネクション切断は、独立的に行われるため、必ずしも順番に行われるわけではない。

【0090】ラインカード1では、TCPコネクションを切断するためのFINセグメントの受信を起因として、TCP管理テーブル4から、コネクション情報を削除する。このコネクション情報の削除は、入力側TCPセグメント管理部2でのみ行う。

【0091】図2の構成例では、クライアント18からのFINセグメント121は、ラインカードA1Aの入力側TCPセグメント管理部2で行う。ラインカードA1Aでは、サーバ19からのFINセグメント123に関しては、何も行わない。また、サーバ19からのFINセグメント123は、ラインカードB1Bの入力側TCPセグメント管理部2で行う。ラインカードB1Bでは、クライアント18からのFINセグメント121に関しては、何も行わない。

【0092】図13は、FINセグメントによる、コネクション情報の削除処理のフローチャートである。但し、FINセグメントによるTCPコネクション切断と、RSTセグメントによるTCPコネクション切断は同一処理であるため、図13の各ステップの説明は、両方の場合について記述する。

【0093】入力側フラグビット判定部51は、TCPセグメント24からフラグビット32を抽出（ステップ131）し、FINビット33とRSTビット35の設定値から、TCPコネクション切断を要求するためのTCPセグメント24であるか否かを確認する（ステップ132）。FINビット33、または、RSTビット35のいずれかがONの場合は、ステップ133に進む。また、FINビット33とRSTビット35の両方がOFFの場合は終了する。但し、入力側フラグビット判定部51に渡されたIPパケットは、4種類（TCPコネクション確立、TCPコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（TCPコネクション確立、データ送信、送達確認）の判定に進むことを意味する。実施の形態4では、FINセグメントは、FINビット33がONであるため、ステップ133に進む。

【0094】入力側コネクション情報管理部54は、IPパケット20内の、送信元IPアドレス26、送信元ポート番号28、送信先IPアドレス27、送信先ポート番号29を組合わせて、コネクション識別子41を生成する（ステップ133）。次に、生成したコネクション識別子41をキーとして、TCP管理テーブル4を検索（ステップ134）し、コネクション情報が既に登録されているか否かを確認する（ステップ135）。

【0095】コネクション情報が既にTCP管理テーブル4に登録されている場合は、現在のTCPコネクションを切断するために、ステップ134で検出した情報をTCP管理テーブル4から削除する（ステップ136）。

【0096】最後に、入力側コネクション情報管理部54で処理されたIPパケット20は、カード間送受信回路9を経由して、そのIPパケット20を送出すべきラインカードに転送される（ステップ137）。

【0097】このように、入力側TCPセグメント管理部2において、FINセグメントの受信を起因として、TCP管理テーブル4からコネクション情報を削除することにより、クライアント18からサーバ19へ、及び、サーバ19からクライアント18への両方向に対応することができる。

【0098】実施の形態5、RSTセグメントによるTCPコネクション切断では、TCPプロトコルで通信する端末間で、1個のセグメントを使用して行う。RSTセグメントは、クライアント18、または、サーバ19のいずれかが、強制的にTCPコネクションを切断する場合に使用する。クライアント18では、TCPプロトコルでの通信を中断する場合に、RSTセグメントを発行する。また、クライアント18がサーバ19の未使用ポート番号に対してコネクション要求した場合、サーバ19は、その要求を拒否するためにRSTセグメントを発行する。

【0099】ラインカード1では、TCPコネクションを切断するためのRSTセグメントの受信を起因として、TCP管理テーブル4から、コネクション情報を削除する。このコネクション情報の削除は、入力側TCPセグメント管理部2と出力側TCPセグメント管理部3の両方で行う。クライアント18からサーバ19に対してRSTセグメントが送信された場合には、ラインカードA1Aの入力側TCPセグメント管理部2とラインカードB1Bの出力側TCPセグメント管理部3が処理を行い、サーバ19からクライアント18に対してRSTセグメントが送信された場合には、ラインカードB1Bの入力側TCPセグメント管理部2とラインカードA1Aの出力側TCPセグメント管理部3が処理を行う。RSTセグメントによるTCPコネクション切断処理のフローは、図13と同一であるため、説明は省略する。

【0100】このように、ラインカードA1A（又はラインカードB1B）では、入力側TCPセグメント管理部2において、RSTセグメントの受信を起因として、TCP管理テーブル4からコネクション情報を削除することにより、クライアント18（又はサーバ19）からの強制的なTCPコネクション切断に対応することができる。また、ラインカードA1A（又はラインカードB1B）では、出力側TCPセグメント管理部3において、RSTセグメントの受信を起因として、TCP管理テーブル4からコネクション情報を削除することにより、サーバ19（又はクライアント18）からの強制的なTCPコネクション切断に対応することができる。

【0101】実施の形態6、本実施の形態では、実施の形態1で示したラインカード1の処理のうち、データ送信の際の処理の詳細を説明する。

【0102】図14は、クライアント18からサーバ19へデータ転送した場合のシーケンスである。サーバ19からクライアント18へデータ転送した場合も同様に動作する。なお、図14において、記述のないFINビット33、SYNビット34、RSTビット35、ACKビット36は、OFFに設定されていることを意味する。

【0103】ユーザデータを転送するTCPセグメント24は、FINビット33、SYNビット34、RSTビット35、ACKビット36のすべてがOFFに設定されている。本明細書では、このTCPセグメント24をTCPデータセグメントと称する。なお、TCPデータセグメントは、データパケットに相当する。また、ユーザデータの送達確認用のTCPセグメント24は、ACKビット36がONに、かつ、FINビット33、SYNビット34、RSTビット35がOFFに設定されている。本明細書では、このTCPセグメント24を送達確認セグメントと称する。なお、送達確認セグメントは、送達確認パケットに相当する。

50 【0104】TCPプロトコルでのデータ転送における

送達確認は、TCPデータセグメント毎に返答する場合と、複数個のTCPデータセグメント毎に返答する場合がある。

【0105】第一に、前者のケースの動作を説明する。まず、第一フェーズとして、クライアント18は、TCPデータセグメント141を、サーバ19に対して送信する。図14の例では、100バイト長のデータを送信する。次に、第二フェーズとして、サーバ19は、クライアント18からのTCPデータセグメント141に対する送達確認セグメント142を、クライアント18に対して送信する。その場合、フラグビット32の内、ACKビット36のみONに設定されている。また、確認応答番号31には、クライアント18からのTCPデータセグメント141のシーケンス番号30にデータサイズを加算した値が設定されている。図14の例では、確認応答番号31は、シーケンス番号30の100にデータサイズの100を加算した200の値が設定される。

【0106】第二に、後者のケースの動作を説明する。まず、第一フェーズとして、クライアント18は、TCPデータセグメント143を、サーバ19に対して送信する。図14の例では、100バイト長のデータを送信する。次に、第二フェーズとして、クライアント18は、サーバからの送達確認を待たずに、ユーザデータを含むTCPセグメント144を、サーバ19に対して送信する。図14の例では、150バイト長のデータを送信する。最後に、第三フェーズとして、サーバ19は、クライアント18からのTCPデータセグメント142までの処理が完了したことを通知するため、送達確認セグメント145を、クライアント18に対して送信する。その場合、フラグビット32の内、ACKビット36のみONに設定されている。また、確認応答番号31には、クライアント18からのTCPデータセグメント144のシーケンス番号30にデータサイズを加算した値が設定されている。図14の例では、確認応答番号31は、シーケンス番号30の300にデータサイズの150を加算した450の値が設定される。

【0107】ラインカード1では、TCPデータセグメントの受信を起因として、入力側TCPセグメント管理部2で、TCPデータセグメントの正当性（連続したデータ列であること）を確認し、中継処理の要否を判断する。また、TCPデータセグメントが正当である場合は、TCP管理テーブル4内の該当するコネクション情報のSeq番号42を更新する。また、ラインカード1では、送達確認セグメントの受信を起因として、出力側TCPセグメント管理部3で、TCP管理テーブル4内の該当するコネクション情報のAck番号43を更新する。

【0108】図15は、TCPデータセグメントに対する処理のフローチャートである。

【0109】入力側フラグビット判定部51は、TCP

セグメント24からフラグビット32を抽出（ステップ151）し、TCPデータセグメントであるか否かを確認する（ステップ152）。TCPデータセグメントでない場合は終了する。但し、入力側フラグビット判定部51に渡されたIPパケットは、4種類（TCPコネクション確立、TCPコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（TCPコネクション確立、TCPコネクション切断、送達確認）の判定に進むことを意味する。実施の形態6では、TCPデータセグメントであるため、ステップ153に進む。

【0110】入力側コネクション情報管理部54は、IPパケット20内の、送信元IPアドレス26、送信元ポート番号28、送信先IPアドレス27、送信先ポート番号29を組合せて、コネクション識別子41を生成する（ステップ153）。次に、生成したコネクション識別子41をキーとして、TCP管理テーブル4を検索（ステップ154）し、一致するコネクション識別子が登録されているか否かを確認する（ステップ155）。TCP管理テーブル4に登録されていない場合は、ステップ163に進む。

【0111】コネクション識別子が登録されているケースとしては、TCPプロトコルでは、TCPデータセグメントの送信側（図14の場合ではクライアント18）が一定期間を超過しても送達確認を受けない場合がある。このとき、送信側はTCPデータセグメントを再送する。しかし、送信側が送達確認を受けない要因には、IPパケット20がネットワークのどこかで廃棄された場合や、IPパケット20の転送遅延が送信側の許容時間を超えた場合など様々である。ステップ155～158は、受信側（図14の場合ではサーバ19）で受け取り済であるTCPデータセグメントに関しては再送の必要がないため、フィルタ部52は、それらのTCPデータセグメントを検出して廃棄することを目的としている。

【0112】ステップ155でYesの場合、フィルタ部52は、まず、TCPデータセグメントのシーケンス番号30と、ステップ154で検出したコネクション情報のAck番号43を比較（ステップ156）し、TCPデータセグメントのシーケンス番号30が、コネクション情報のAck番号43より小さいか確認する（ステップ157）。TCPデータセグメントのシーケンス番号30が、コネクション情報のAck番号43より小さい場合、そのTCPデータセグメントは受信側で受け取り済であることを示すため、TCPデータを廃棄する（ステップ158）。

【0113】TCPプロトコルでは、連続したTCPデータセグメントの一部が抜けた場合、受信側は抜けたTCPデータセグメントからの再送を、送信側に対して要求する。そのため、連続したTCPデータセグメントの

内、一つのTCPデータセグメントが抜けた時点で、それに続くTCPデータセグメントは意味を持たない。フィルタ部52では、TCPデータセグメントの抜けを検出して、それ以降のTCPデータセグメントを廃棄することを目的としている。

【0114】ステップ157でNoの場合、フィルタ部52は、まず、TCPデータセグメントのシーケンス番号30と、ステップ154で検出したコネクション情報のSeq番号42を比較（ステップ159）し、TCPデータセグメントのシーケンス番号30が、コネクション情報のSeq番号42より大きいか確認する（ステップ160）。TCPデータセグメントのシーケンス番号30が、コネクション情報のSeq番号42より大きい場合、TCPデータセグメントの抜けが起きていることを示すため、TCPデータを廃棄する（ステップ161）。

【0115】ステップ160でNoの場合、Seq番号更新部53は、ステップ154で検出したコネクション情報のSeq番号42に、TCPデータセグメントのデータサイズを加算する（ステップ162）。ここで更新されたSeq番号42の値は、次のTCPデータセグメントのシーケンス番号30の値（次中継シーケンス番号）である。

【0116】最後に、Seq番号更新部53で処理されたIPパケット20は、カード間送受信回路9を経由して、そのIPパケット20を送出すべきラインカード1B～1Dに転送される（ステップ163）。

【0117】図16は、送達確認セグメントに対する処理のフローチャートである。

【0118】出力側フラグビット判定部61は、TCPセグメント24からフラグビット32を抽出（ステップ171）し、送達確認セグメントであるか否かを確認する（ステップ172）。送達確認セグメントでない場合は終了する。但し、出力側フラグビット判定部61に渡されたIPパケットは、4種類（TCPコネクション確立、TCPコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（TCPコネクション確立、TCPコネクション切断、データ送信）の判定に進むことを意味する。実施の形態6では、送達確認セグメントであるため、ステップ173に進む。

【0119】出力側コネクション情報管理部63は、IPパケット20内の、送信先IPアドレス27、送信先ポート番号29を組合せて、送信元ID45を生成する（ステップ173）。また、IPパケット20内の、送信元IPアドレス26、送信元ポート番号28を組合せて、送信先ID46を生成する（ステップ174）。そして、ステップ173で生成した送信元ID45と、ステップ174で生成した送信先ID46を組合せて、コネクション識別子41を算出する（ステップ

175）。出力側コネクション情報管理部63では、入力側コネクション情報管理部54と異なり、IPパケット20内の送信元/送信先を反転して、コネクション識別子41を生成する。次に、生成したコネクション識別子41をキーとして、TCP管理テーブル4を検索（ステップ176）し、一致するコネクション識別子が既に登録されているか否かを確認する（ステップ177）。登録されている場合はステップ178に進み、登録されていない場合はステップ179に進む。

【0120】ステップ177でYesの場合は、Ack番号更新部62は、ステップ176で検出したコネクション情報のAck番号43に、送達確認セグメントの確認応答番号31の値を設定する（ステップ178）。ここで更新されたAck番号43の値は、送信側が次に送信するTCPセグメント24のシーケンス番号30の値であり、このシーケンス番号30未満のTCPデータセグメントは受信側で受け取り済みであることを示す。

【0121】最後に、Ack番号更新部62で処理されたIPパケット20は、レイヤ2/3処理部8に渡される（ステップ179）。

【0122】図17は、クライアント18からサーバ19に対して、2個の連続したデータA～データBを送信する場合の例である。ここで、サーバ19からの送達確認セグメント183が何らかの要因により転送遅延が大きくなり、クライアント18がデータAを含むTCPデータセグメントを再送したと仮定する。なお、図17におけるTCPデータセグメントのデータサイズは、すべて50バイトとする。

【0123】図17を用いて、具体的な動作を説明する。IPルータ10は、データAを含むTCPデータセグメント181、及び、データBを含むTCPデータセグメント182に対するサーバ19からの送達確認セグメント183を受信した時点で、TCP管理テーブル4内の該当するコネクション情報のAck番号43を200に設定する。その結果、ルータ10は、次のTCPセグメント24のシーケンス番号30は200であると予測する。しかし、ルータ10は、クライアント18から再送されたデータAを含むTCPデータセグメント184を受信するため、TCPデータセグメント184のシーケンス番号30とコネクション情報のAck番号43を比較した結果、データ重複と判定し、ルータ10内で廃棄する。なお、既存の方式では、TCPデータセグメント184はルータ10で廃棄されず、サーバ19まで転送され、サーバ19で廃棄するため、ルータ10とサーバ19の間のネットワークに無効なトラフィックが流れることになる。

【0124】このように、ルータ10内のラインカード1において、出力側TCPセグメント管理部3でコネクション情報のAck番号43を管理して、TCPプロトコル通信における受信側が受け取り済みのTCPセグメ

ント24を把握することにより、従来は受信端末で廃棄していたデータをルータ10内のラインカード1（入力側TCPセグメント管理部2）で早期検出して廃棄することにより、データ重複による無効なトライフィックを削減することができる。

【0125】図18は、クライアント18からサーバ19に対して、4個の連続したデータA～データDを送信する場合の例である。ここで、クライアント18とルータ10の間のネットワークにおいて、データBを含むTCPセグメント182が廃棄されたと仮定する。なお、図18におけるTCPデータセグメントは、すべて50バイトとする。

【0126】図18を用いて、具体的な動作を説明する。まず、ルータ10は、クライアント18からのデータAを含むTCPデータセグメント191を受信すると、TCP管理テーブル4内の該当するコネクション情報のSeq番号42を150に設定し、次のTCPセグメント24のシーケンス番号30は150であると予測する。しかし、ルータ10は、クライアント18から次にデータCを含むTCPデータセグメント193を受信するため、TCPデータセグメント193のシーケンス番号30とコネクション情報のSeq番号42を比較した結果、データ抜けと判定し、ルータ10内で廃棄する。なお、既存の方式では、サーバ19までTCPデータセグメント193～194は転送され、サーバ19で廃棄するため、ルータ10とサーバ19の間のネットワークに無効なトライフィックが流れることになる。また、後続するデータDを含むTCPデータセグメント194に対しても、同様に廃棄する。

【0127】サーバ19は、クライアント18からのデータAを含むTCPデータセグメント191は正常に受信したため、送達確認セグメント195をクライアント18に送信する。クライアント18では、送達確認セグメント195を受信した後、TCPデータセグメント192～194に対する送達確認がないため、一定時間を経過すると、データB～データDを含むTCPデータセグメント196～198を再送する。

【0128】サーバ19は、クライアント18からのデータB～データDを含むTCPデータセグメント196～198を正常に受信したため、送達確認セグメント199をクライアント18に送信する。

【0129】このように、ルータ10内のラインカード1において、入力側TCPセグメント管理部2でコネクション情報のSeq番号42を管理して、ラインカード1が次に受信するTCPセグメント24を予測することにより、従来は受信端末で廃棄していたデータをルータ10内のラインカード1（入力側TCPセグメント管理部2）で早期検出して廃棄することにより、データ抜けによる無効なトライフィックを削減することができる。

【0130】また、データ重複やデータ抜けによる無効

なトライフィックを削減することにより、ネットワークにおける幅轍が減り、ネットワーク全体の利用効率を向上させることができる。

【0131】なお、以上の実施の形態1～6では、中継処理装置の例としてラインカードを用いた場合について説明したが、これに限るものではなく、実施の形態1～6に示した処理を実現できるものであれば、ラインカード以外のものでもよい。

【0132】また、以上の実施の形態1～6では、TCPプロトコルを利用するIPパケットを前提として説明したが、これに限るものではなく、他の通信プロトコルを利用するデータにも適用することができる。

【0133】また、以上の実施の形態1～6では、本発明に係る中継処理装置について説明したが、実施の形態1～6に示した処理手順と同様の手順により、本発明に係る中継処理方法も実現することができる。

【0134】ここで、実施の形態1～6で示したラインカードの特徴を以下にて再言する。

【0135】実施の形態1～6のラインカードは、LANまたはWANに接続されるラインカードにおいて、單一方向のTCPコネクション毎に、コネクション情報を管理するTCP管理テーブルと、LANまたはWANから受信したIPパケットのトランスポート層のプロトコル種別を判別して、前記トランスポート層にTCPプロトコルを使用する前記IPパケットを入力側TCPセグメント管理部に渡し、それ以外の前記IPパケットをそのまま中継する入力フレーム種別判定部と、前記入力フレーム種別判定部から渡された前記トランスポート層にTCPプロトコルを使用する前記IPパケットを受け、前記TCP管理テーブルの制御、及び、TCPセグメントの正当性の確認を行う入力側TCPセグメント管理部と、他のラインカードから中継されたIPパケットのトランスポート層のプロトコル種別を判別して、前記トランスポート層にTCPプロトコルを使用する前記IPパケットを出力側TCPセグメント管理部に渡し、それ以外の前記IPパケットをそのまま中継する出力フレーム種別判定部と、前記出力フレーム種別判定部から渡された前記トランスポート層にTCPプロトコルを使用する前記IPパケットを受けて、前記TCP管理テーブルの制御を行う出力側TCPセグメント管理部と、を備えたことを特徴とする。

【0136】実施の形態1～6のラインカードは、單一方向のTCPコネクション毎に、送信元のTCPソケットと送信先のTCPソケットを組合せたコネクション識別子と、前記ラインカードが次に受信するデータ送信用TCPセグメントのシーケンス番号を記録するSeq番号と、前記ラインカードが受信した最新の送達確認用TCPセグメントの確認応答番号を記録するAck番号と、前記コネクション識別子と前記Seq番号と前記Ack番号を組合せた情報であるコネクション情報の有効

性を示す確立フラグから構成されるTCP管理テーブルと、を有することを特徴とする。

【0137】実施の形態1～6のラインカード内の入力側TCPセグメント管理部は、トランスポート層にTCPプロトコル層を使用するIPパケットのフラグビットにより、前記IPパケット内のTCPセグメントの種別を判定する入力側フラグビット判定部と、前記入力側フラグビット判定部で、TCPコネクション確立用またはTCPコネクション切断用と判定された前記TCPセグメントの内容に基づき、前記TCP管理テーブルに前記コネクション情報を登録または削除する入力側コネクション情報管理部と、前記入力側フラグビット判定部で、データ送信用と判定された前記TCPセグメントに関して、前記TCP管理テーブルを参照して、前記TCPセグメントの正当性を確認するフィルタ部と、前記入力側フラグビット判定部で、データ送信用と判定された前記TCPセグメントの内容に基づき、前記TCP管理テーブル内の該当する前記コネクション情報のSeq番号を更新するSeq番号更新部と、定期的に前記TCP管理テーブルの前記確立フラグを監視し、前記コネクション情報の有効性を確認するコネクション確認部と、を有することを特徴とする。

【0138】実施の形態1～6のラインカード内の出力側TCPセグメント管理部は、トランスポート層にTCPプロトコル層を使用するIPパケットのフラグビットにより、前記IPパケット内のTCPセグメントの種別を判定する出力側フラグビット判定部と、前記出力側フラグビット判定部で、TCPコネクション確立用またはTCPコネクション切断用と判定された前記TCPセグメントの内容に基づき、前記TCP管理テーブルに前記コネクション情報を登録または削除する出力側コネクション情報管理部と、前記出力側フラグビット判定部で、送達確認用と判定された前記TCPセグメントの内容に基づき、前記TCP管理テーブル内の該当する前記コネクション情報のAck番号を更新するAck番号更新部と、を有することを特徴とする。

【0139】実施の形態2のラインカードは、TCPコネクション確立シーケンスの第一フェーズにおける、クライアントがTCPコネクションを確立するためのTCPセグメントであるSYNセグメントの受信を起因とし、前記入力側TCPセグメント管理部で、前記TCP管理テーブルへの前記コネクション情報の登録を行い、前記出力側TCPセグメント管理部で、前記コネクション情報の有効化を行うことを特徴とする。

【0140】実施の形態2のラインカードは、定期的に前記TCP管理テーブルの前記確立フラグを監視し、TCPプロトコル通信を行う端末間で、双方向のTCPコネクションの確立していない前記コネクション情報を削除することを特徴とする。

【0141】実施の形態3のラインカードは、TCPコ

ネクション確立シーケンスの第二フェーズにおける、サーバがTCPコネクションを確立するためのTCPセグメントであるSYNセグメントの受信を起因とし、前記入力側TCPセグメント管理部で、前記TCP管理テーブルへの前記コネクション情報の登録、及び、前記コネクション情報の有効化を同時にを行うことを特徴とする。

【0142】実施の形態4、5のラインカードは、クライアントがTCPコネクションを切断するためのTCPセグメントであるFINセグメント、または、クライアントがTCPコネクションを強制的に切断するためのTCPセグメントであるRSTセグメントの受信を起因とし、前記入力側TCPセグメント管理部で、前記FINセグメントまたは前記RSTセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記TCP管理テーブル内から該当する前記コネクション情報を特定し、前記TCP管理テーブルから前記コネクション情報を削除することを特徴とする。

【0143】実施の形態5のラインカードは、サーバがTCPコネクションを強制的に切断するためのTCPセグメントであるRSTセグメントの受信を起因とし、前記出力側TCPセグメント管理部で、前記RSTセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記TCP管理テーブル内から該当する前記コネクション情報を特定し、前記TCP管理テーブルから前記コネクション情報を削除することを特徴とする。

【0144】実施の形態6のラインカードは、ユーザデータを含むTCPセグメントであるTCPデータセグメントの受信を起因とし、前記入力側TCPセグメント管理部で、前記TCPデータセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記TCP管理テーブル内から該当する前記コネクション情報を特定し、前記コネクション情報のSeq番号を、前記TCPデータセグメントのデータサイズを加算した値に更新することを特徴とする請求項1に記載の通信パケット制御方式。

【0145】実施の形態6のラインカードは、前記TCPデータセグメントの送達確認用のTCPセグメントである送達確認セグメントの受信を起因とし、前記出力側TCPセグメント管理部で、前記送達確認セグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記TCP管理テーブル内から該当する前記コネクション情報を特定し、前記コネクション情報のAck番号を、前記送達確認セグメントの確認応答番号の値に更新することを特徴とする。

【0146】実施の形態6のラインカードは、ユーザデータを含むTCPセグメントであるTCPデータセグメントに関して、前記入力側TCPセグメント管理部で、前記TCPデータセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記TCP

P管理テーブル内から該当する前記コネクション情報を特定し、前記コネクション情報のA ck番号と、前記TCPデータセグメントのシーケンス番号を比較して、受信側で受け取り済みのTCPデータセグメントを検出し、前記受信側で受け取り済みのTCPデータセグメントを廃棄することを特徴とする。

【0147】実施の形態6のラインカードは、ユーザータを含むTCPセグメントであるTCPデータセグメントに関して、前記入力側TCPセグメント管理部で、前記TCPデータセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記TCP管理テーブル内から該当する前記コネクション情報を特定し、前記コネクション情報のSeq番号と、前記TCPデータセグメントのシーケンス番号を比較して、連続した前記TCPデータセグメントの一部が抜けたことを検出し、抜けた前記TCPデータセグメントに続く前記TCPデータセグメントを廃棄することを特徴とする。

【0148】

【発明の効果】本発明によれば、データパケットが受信される度に、中継要否判断部がデータパケットの送信シーケンス番号と通信管理テーブルに記憶された判断基準シーケンス番号とを比較して中継処理の要否判断を行うため、従来はパケット受信側で破棄していた無効なデータパケットを早期に検出することができ、これにより無効なデータパケットの中継を削減することができる。ネットワークにおける幅轍を減らし、ネットワーク全体の利用効率を向上させることができる。

【0149】また、本発明によれば、中継要否判断部は次中継シーケンス番号を算出し、通信管理テーブルは次中継シーケンス番号のうち最新の次中継シーケンス番号を記憶し、中継要否判断部はデータパケットの送信シーケンス番号と通信管理テーブルに記憶された次中継シーケンス番号とを比較して中継処理の要否判断を行うため、従来はパケット受信側で破棄していたデータ抜けによる無効なデータパケットを早期に検出することができ、これにより無効なデータパケットの中継を削減することが可能となり、ネットワークにおける幅轍を減らし、ネットワーク全体の利用効率を向上させることができる。

【0150】また、本発明によれば、通信管理テーブルは確認シーケンス番号のうち最新の確認シーケンス番号を記憶し、中継要否判断部はデータパケットの送信シーケンス番号と通信管理テーブルに記憶された確認シーケンス番号とを比較して中継処理の要否判断を行うため、従来はパケット受信側で破棄していたデータ重複による無効なデータパケットを早期に検出することができ、これにより無効なデータパケットの中継を削減する可能となり、ネットワークにおける幅轍を減らし、ネットワーク全体の利用効率を向上させることができる。

【0151】また、本発明によれば、通信管理テーブルは次中継シーケンス番号と確認シーケンス番号とをコネクション識別子情報に対応づけて記憶し、中継要否判断部は、コネクション識別子情報に基づき対応する次中継シーケンス番号と確認シーケンス番号とを特定し、特定した次中継シーケンス番号及び確認シーケンス番号とデータパケットの送信シーケンス番号とを比較するため、双方向の通信コネクションのうち單一方向の通信コネクション単位でデータ抜けやデータ重複を検出することができ、ネットワークにおける幅轍を減らし、ネットワーク全体の利用効率を向上させることができる。

【0152】また、本発明によれば、通信管理テーブルはコネクション設定パケットの受信時にコネクション識別子情報を記憶し、コネクション管理部は応答コネクション設定パケットの受信時に通信コネクションの確立の判断を行うため、以降のデータパケットの中継処理要否判断において双方向の通信コネクションのうち單一方向の通信コネクション単位でデータ抜けやデータ重複を検出することができ、ネットワークにおける幅轍を減らし、ネットワーク全体の利用効率を向上させることができる。

【0153】また、本発明によれば、コネクション確認部が一定周期ごとに通信管理テーブルを検査して無効なコネクション識別子情報を削除するため、通信管理テーブルのリソースの浪費を防止することができる。

【0154】また、本発明によれば、コネクション管理部は応答コネクション設定パケットの受信時にコネクション識別子情報の登録と通信コネクションの確立の判断を行うため、コネクション識別子情報が無効な期間が存在せず、コネクション確立有無の確認処理を不要とすることができる。

【0155】本発明によれば、コネクション管理部は特定ネットワーク通信装置よりコネクション切断パケットを受信した場合に、対応するコネクション識別子情報を通信管理テーブルより削除するため、特定ネットワーク通信装置からのコネクション切断要求に対応することができる。

【0156】本発明によれば、コネクション管理部は特定ネットワーク通信装置よりコネクション強制切断パケットを受信した場合に、対応するコネクション識別子情報を通信管理テーブルより削除するため、特定ネットワーク通信装置からのコネクション強制切断要求に対応することができる。

【0157】本発明によれば、コネクション管理部は他ネットワーク通信装置よりコネクション強制切断パケットを受信した場合に、対応するコネクション識別子情報を通信管理テーブルより削除するため、他ネットワーク通信装置からのコネクション強制切断要求に対応することができる。

【図面の簡単な説明】

【図 1】 実施の形態 1～6 のネットワーク構成例を示す図。

【図 2】 ラインカードの内部構成例を示す図。

【図 3】 IP パケットのデータ構成例を示す図。

【図 4】 IP パケット内のフラグビットのデータ構成例を示す図。

【図 5】 TCP 管理テーブルの構成例を示す図。

【図 6】 ラインカード内の入力側 TCP セグメント管理部の内部構成例を示す図。

【図 7】 ラインカード内の出力側 TCP セグメント管理部の内部構成例を示す図。

【図 8】 コネクション確立時の通信シーケンスを示す図。

【図 9】 コネクション確立時のラインカード内の入力側 TCP セグメント管理部の処理を示すフローチャート図。

【図 10】 コネクション確立時のラインカード内の出力側 TCP セグメント管理部の処理を示すフローチャート図。

【図 11】 ラインカード内のコネクション確認部の処理を示すフローチャート図。

【図 12】 コネクション切断時の通信シーケンスを示す図。

【図 13】 コネクション切断時のラインカード内の入

力側 TCP セグメント管理部の処理を示すフローチャート図。

【図 14】 データ送信時の通信シーケンスを示す図。

【図 15】 データ送信時のラインカード内の入力側 TCP セグメント管理部の処理を示すフローチャート図。

【図 16】 データ送信時のラインカード内の出力側 TCP セグメント管理部の処理を示すフローチャート図。

【図 17】 データ送信時の通信シーケンスを示す図。

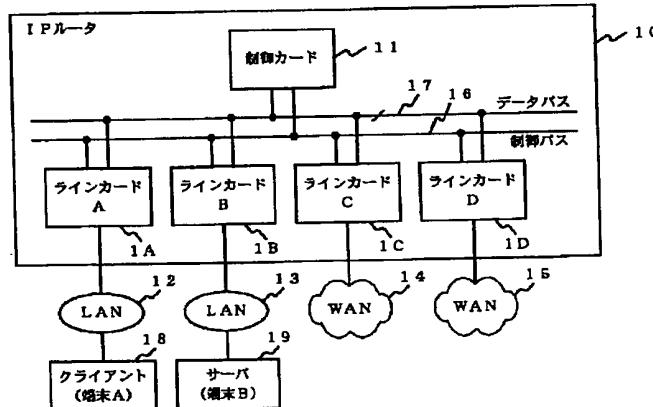
【図 18】 データ送信時の通信シーケンスを示す図。

【図 19】 従来の技術を示す図。

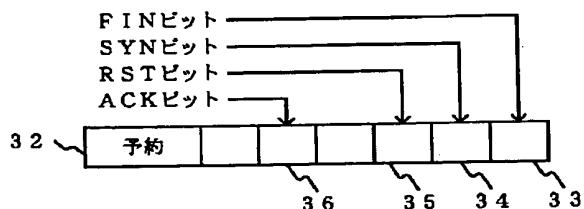
【符号の説明】

1 ラインカード、2 入力側 TCP セグメント管理部、3 出力側 TCP セグメント管理部、4 TCP 管理テーブル、5 入力フレーム種別判定部、6 出力フレーム種別判定部、7 ネットワーク送受信回路、8 レイヤ 2/3 处理部、9 カード間送受信回路、10 IP ルータ、11 制御カード、12 LAN、13 LAN、14 WAN、15 WAN、16 制御バス、17 データバス、18 クライアント、19 サーバ、51 入力側フラグビット判定部、52 フィルタ部、53 Seq 番号更新部、54 入力側コネクション情報管理部、55 コネクション確認部、61 出力側フラグビット判定部、62 Ack 番号更新部、63 出力側コネクション情報管理部。

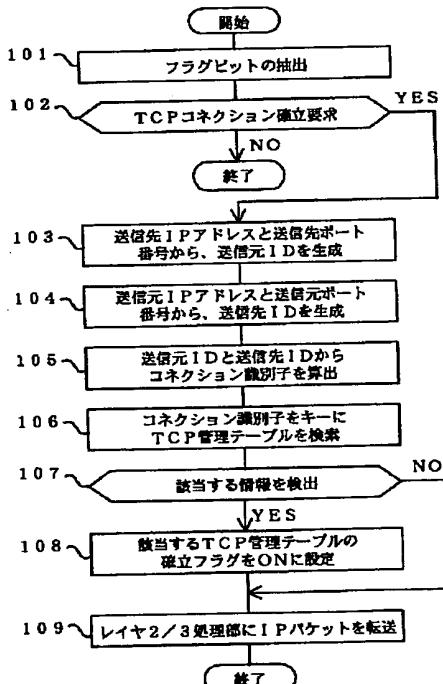
【図 1】



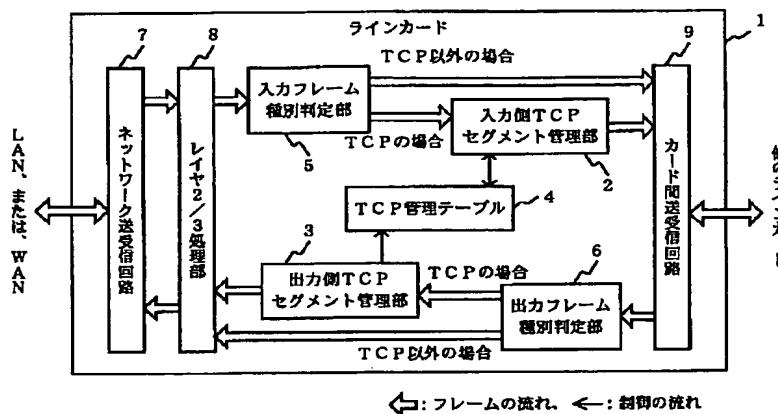
【図 4】



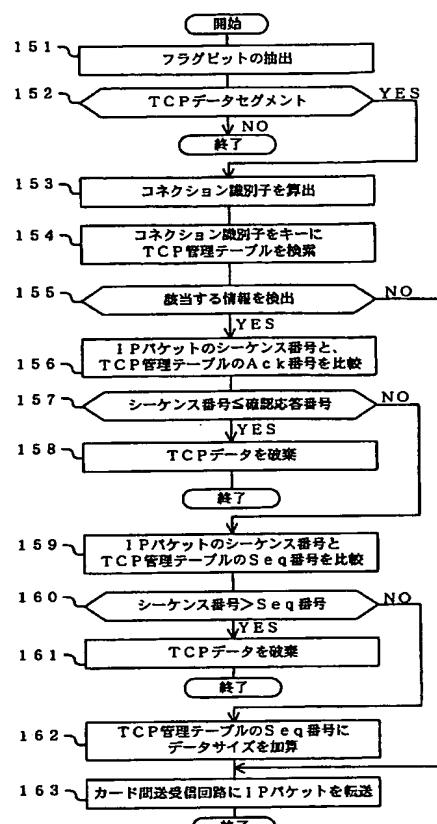
【図 10】



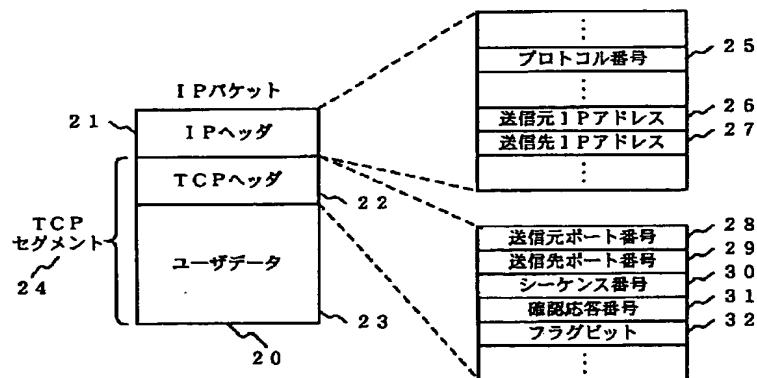
【図2】



【図15】



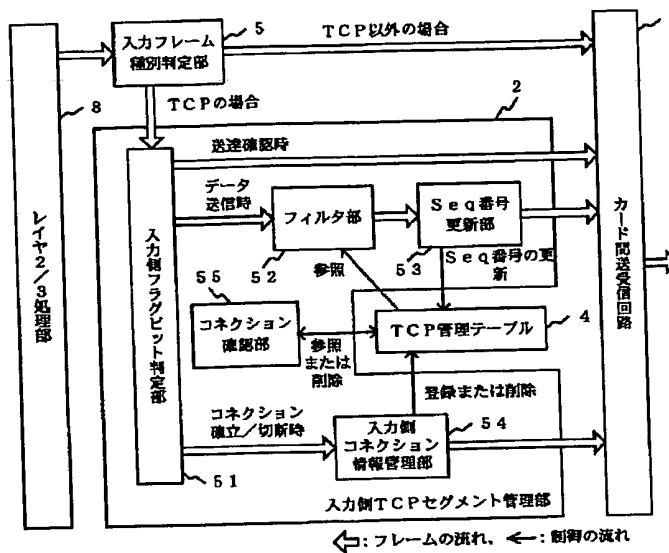
【図3】



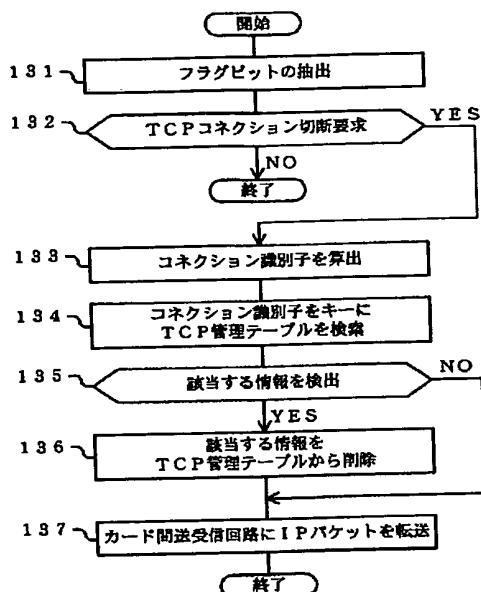
【図5】

41	42	43	44
45	46	47	48
コネクション識別子			
送信元ID	送信先ID	Seq番号	Ack番号
端末AポートX	端末BポートY	12	10
端末BポートW	端末AポートZ	138	138
⋮	⋮	⋮	⋮
			確立フラグ
			ON
			OFF

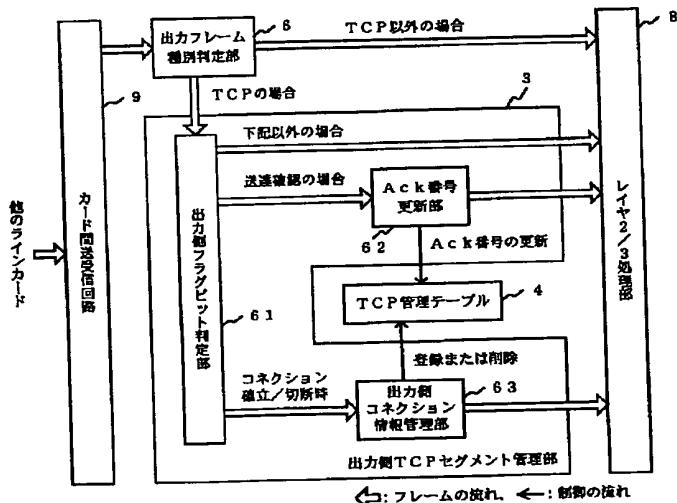
【図6】



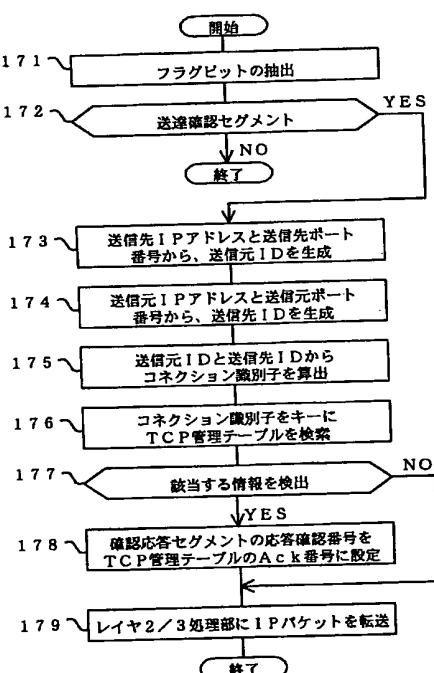
【図13】



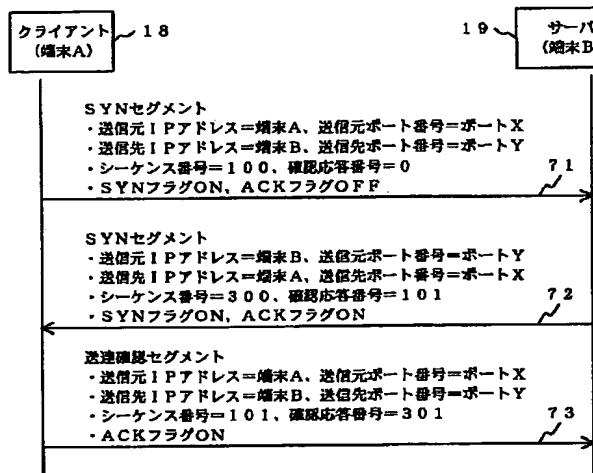
【図7】



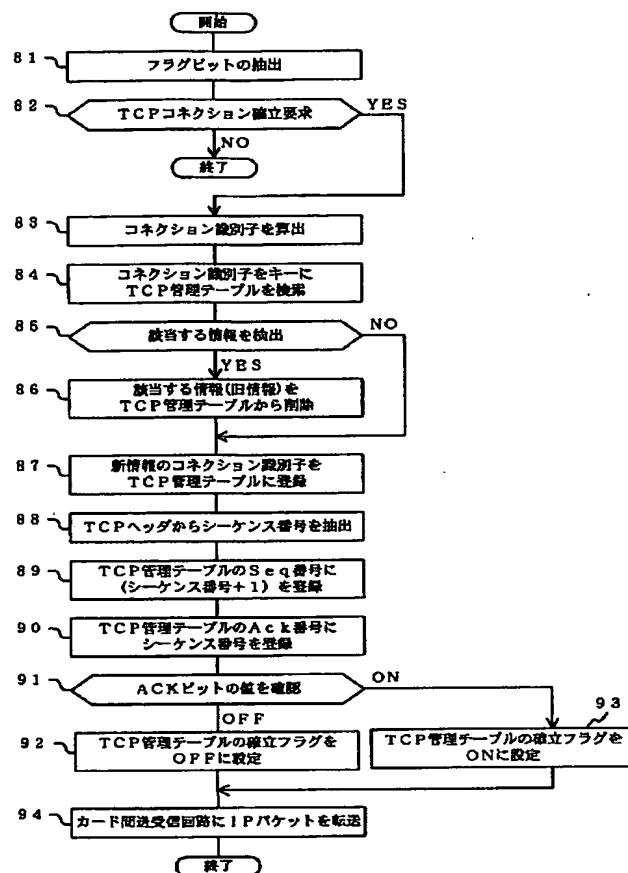
【図16】



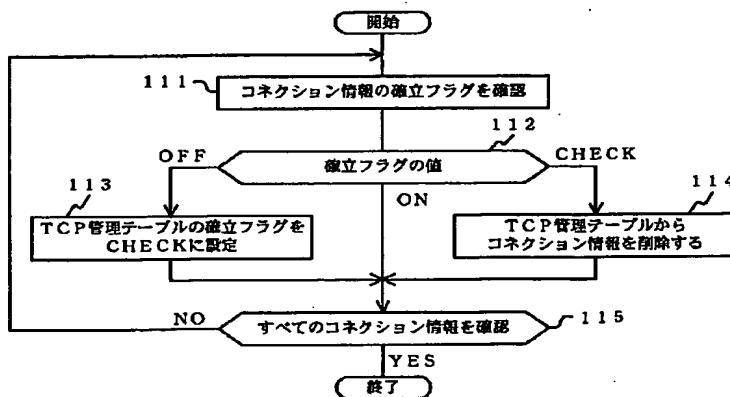
【図8】



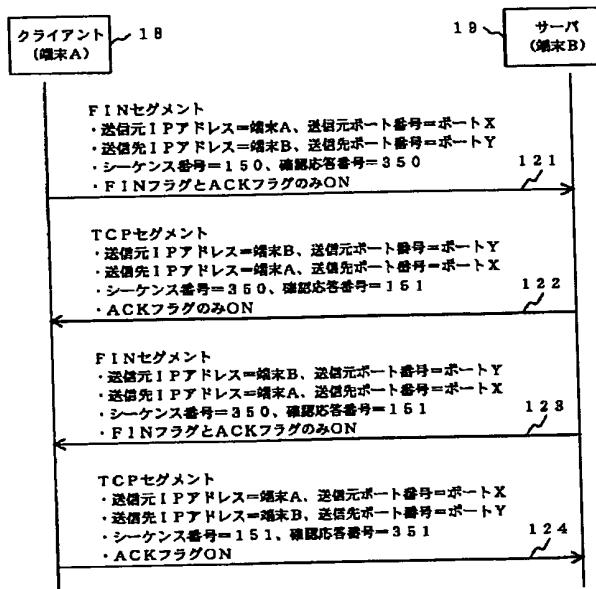
【図9】



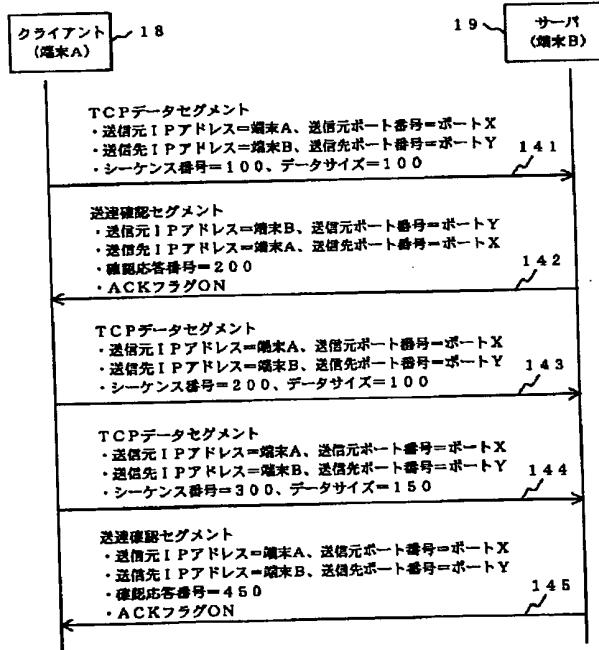
【図11】



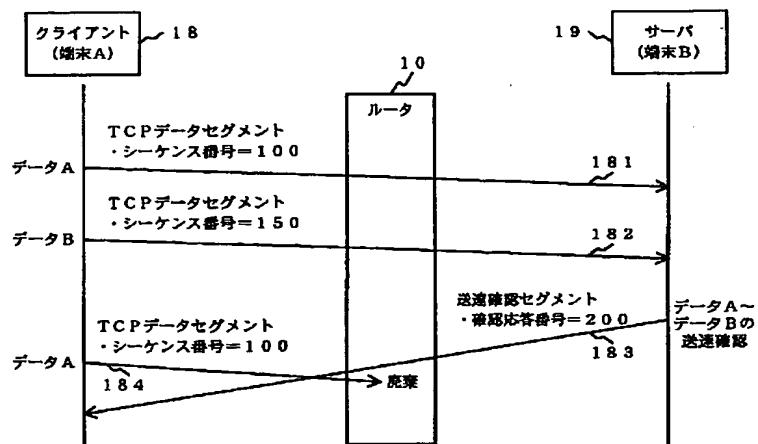
【図12】



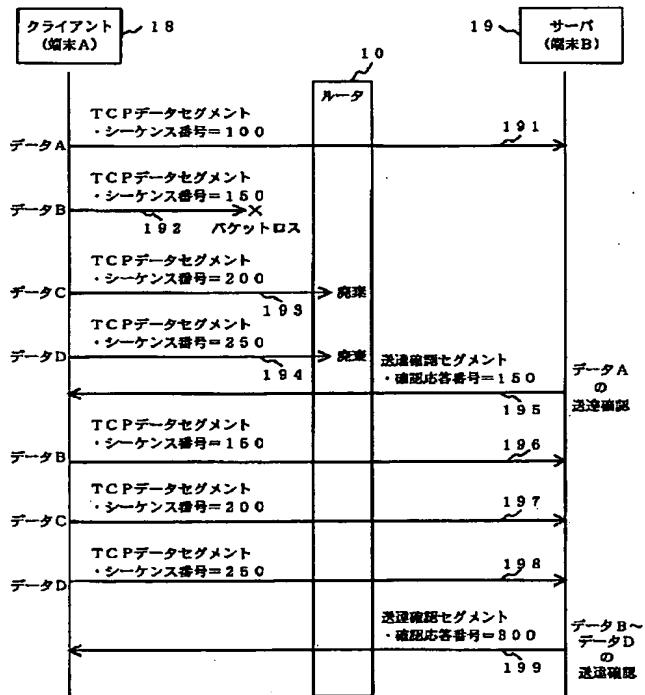
【図14】



【図17】



【図18】



【図19】

